Syllabus for Math 593
Fall Term 2018
Classes MWF 2-3, 3866 East Hall

Instructor: Stephen DeBacker
Office: 4076 East Hall
Phone: 724-763-3274
e-mail: smdbackr@umich.edu

Office hours: M 9-10pm; W 4-5pm; Th 9:30-10:30pm

Texts/Resources:

A: Aluffi, P. *Algebra: Chapter 0*, Graduate Studies in Mathematics, AMS, Providence, 2009, ISBN: 978-0821847817

C1: Conrad, K. *Tensor Products*. [1]

C2: Conrad, K. *Tensor Products II*. [2]

DF: Dummit, D. and R. Foote. *Abstract Algebra*, Third Edition. Wiley, 2004. ISBN: 978-0471433347.

HK: Hoffman, Kenneth and R. Kunze, *Linear algebra*, Second edition. Prentice-Hall, 1971. ISBN: 978-0135367971

L: Lang, S. *Algebra*, Revised 3rd edition. Graduate Texts in Mathematics. Springer, 2002. ISBN: 978-0-387-95385-4.[3]

Philosophy: "He was not fast. Speed means nothing. Math doesn't depend on speed. It is about deep." (Yuriu Burago commenting on Fields Medal winner Grigory Perelman in Sylvia Nasar and David Gruber, *Manifold Destiny*, The New Yorker, August 28, 2006, pp. 44–57.)

An Overview: It is assumed that you have acquired a solid foundation in the theoretical aspects of linear algebra. In particular, you should know the material of [DF04, §§11.1–11.4] thoroughly. It is also assumed that you have been through a serious undergraduate abstract algebra course.

Pedagogy: This course will be taught in an Inquiry Based Learning style, a teaching method that "emphasizes discovery, analysis and investigation to deepen students' understanding of the material and its applications."[4] There will be very little lecture; instead, you will work through worksheets[5] that guide you as you learn and internalize the material.

Nota bene: Even if I were to lecture, there is absolutely no way that I could cover everything that we expect you to learn in this class. So, do your reading and learn the material there.

Grade: 60% of your grade will be determined by the effort you put into your homework, worksheets, and group work. Honest effort will result in full marks. Group work will have two components: groups will be responsible for TEXing up solutions to the worksheets and they will be responsible for creating official TEXed solutions to the homeworks. I have never done this before, so there may be modifications. However, any modifications will be consistent with the following: (a) I do not want to reward cheaters, and (b) I do not want to favor those arriving with stronger mathematical backgrounds.

There will also be a midterm exam counting 15% and a final counting 25%. The midterm will probably occur on October 19. It appears that the registrar has scheduled the final for Wednesday, December 19, from 10:30 to 12:30. Please verify this on your own. All exams are modified take home exams.

Homework: Homework will usually be assigned every Friday. The main part will be due at the beginning of class on the following Friday. The linear algebra review part (Monday Homework) will usually be due on the Monday that falls ten days after it is assigned. Problems with one star do not need to be handed in, but you had better know how to do them. Bonus problems are just that; they do not need to be handed in.

To facilitate the grading of homework: do the problems in order, write on only one side of the paper, and use standard sized paper. No credit will be given if you misstate a problem, so pay attention. You are encouraged to discuss the problems with other students, but you must write up your solutions independently. Warning: It is unbelievable easy to

[1] Available at: http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/tensorprod.pdf

[2] Available at: http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/tensorprod2.pdf

[3] A free electronic edition is available at:
https://link-springer-com.proxy.lib.umich.edu/content/pdf/10.1007%2F978-1-4613-0041-0.pdf

[4] https://lsa.umich.edu/math/centers-outreach/ibl-center-for-inquiry-based-learning.html

[5] These worksheets are very rough. Every time I look at them I identify new, egregious errors for which my PhD should be revoked. I expect that you will as well.

detect plagiarism in mathematics; if you are caught, you will fail. Your solutions should be understandable to your peers; that is, your solutions should be correct, complete, and justified. Late homework will not be accepted (it receives a zero).

Waiting to begin your homework until the evening before it is due is an extremely bad idea.

Exams: There are no alternate or makeup exams (except in cases of extreme human tragedy). The exams will be based entirely on homework, class work (notes/worksheets), and True/False questions. In other words: do your homework and *understand* it and review your notes/worksheets and *understand* them.

Accommodations for a disability: If you think you need an accommodation for a disability, please let me know as soon as possible. In particular, a Verified Individualized Services and Accommodations (VISA) form must be provided to me at least two weeks prior to the need for a test/quiz accommodation. The Services for Students with Disabilities (SSD) Office (G664 Haven Hall; `http://ssd.umich.edu/`) issues VISA forms.

Student Responsibilities: Experience shows that students who attempt a substantial portion of their written homework the day it is assigned do quite well in their math courses.

Climate: Each of you deserves to learn in an environment where you feel safe and where you are respected.

The climate in the mathematical community at Michigan is heavily influenced by the students in it; this now includes you. Our choices directly affect, for good and/or bad, the health of the communities in which we live and work, please choose to build and maintain a welcoming, thriving mathematical community.

Please politely call out your peers and professors on inappropriate behavior. Examples of inappropriate behavior include parading one's knowledge of advanced mathematics, dismissing others' questions as trivial, and any disparaging comments about other students' abilities, grades, appearance, course selection, likelihood to date, likelihood to get tenure, mathematical tastes, etc. If you don't feel comfortable doing this, then talk to me or some university official that you trust (e.g., your advisor, the university ombudsperson, ...).

Finally, mathematics requires the courage to take risks – intellectually, socially, emotionally, ... In particular, many of us find it unnerving to share our mathematical ideas, especially those we are not sure are correct, with others. In order to develop our capacity for taking these risks, we must respect and support each other.

QR Exams: Math 593 and 594 provide excellent preparation for the QR exams. However, neither is a QR prep class; for test prep I recommend looking at Mel Hochster's excellent review notes[1] and the Department's archive of past QR exams.[2]

Thanks: The worksheets/homework of this course are the product of time spent with a host of algebra books, Internet sites, and colleagues. I thank Pete Clark, Brian Conrad, Keith Conrad, Matt Emerton, and David Speyer for writing enlightening and clear blurbs, posts, and documents. I thank Karen Smith for sharing her Fall 2014 Math 593 materials.[3] I thank Aniruddh Agarwal, Ryan Britton, Amanda Burcroff, Zhou Fang, Vignesh Jagathese, David Jin, Jaeyoon Kim, Zachary Luallen, Steffen Maass, Malavika Mukundan, Yuping Ruan, Matthew Sawoski, Zheng Yang, and Juntai Zhou for the many improvements to these worksheets and homeworks that they recommended.
Outside of the many mistakes and obfuscations I have introduced, nothing here is original.

REFERENCES

[A09] Paolo Aluffi. *Algebra: chapter 0*. Vol. 104. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2009, pp. xx+713. ISBN: 978-0-8218-4781-7.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[J85] Nathan Jacobson. *Basic algebra. I*. Second. W. H. Freeman and Company, New York, 1985, pp. xviii+499. ISBN: 0-7167-1480-9.

[Jac89] Nathan Jacobson. *Basic algebra. II*. Second. W. H. Freeman and Company, New York, 1989, pp. xviii+686. ISBN: 0-7167-1933-9.

[Lan02] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, pp. xvi+914. ISBN: 0-387-95385-X.

[1] See "VIGRE Algebra QR Review Material" at `http://www.math.lsa.umich.edu/~hochster/`

[2] Available at `http://dept.math.lsa.umich.edu/graduate/qualifiers/`.

[3] Available at `http://www.math.lsa.umich.edu/~kesmith/Math593-2014.html`

Please report any errors you find to smdbackr@umich.edu

Math 593: Tentative day-by-day syllabus			
Week	Monday	Wednesday	Friday
Sep 3 – Sep 7 A: I: 3.1–4.2 DF: 7.1–7.6 L: 2.1–2.4	No class	Introduction: rings, modules, algebras	Rings: products and Chinese Remainder Theorem
Sep 10 – Sep 14 DF: 8.1–8.3 L: 2.5	Rings: quotients and localizations	Rings: UFDs and Noetherian rings	Rings: PIDs and Euclidean domains
Sep 17 – Sep 21 DF: 9.1–9.5, 10.1 L: 4.1 – 4.3	Rings: Gauss' Lemma and reducing polynomials mod I	Polynomials: irreducibility	Modules: the fundamentals
Sep 24 – Sep 28 DF: 10.1–10.3 DF: pp. 378–385 L: 3.4	Modules: direct products and direct sums	Modules: free modules	Modules: more on free modules; finitely generated and presented
Oct 1 – Oct 5 DF: 12.1, 12.2 L: 3.7, 15.1	Modules: presentations	Modules: torsion	Modules: rational canonical form
Oct 8 – Oct 12 DF: 12.3 L: 15.2, 15.3	Modules: Cayley-Hamilton	Modules: Jordan form	Modules: Structure Theorem for Finitely Generated Modules over a PID
Oct 15 – Oct 19	No Class – Fall Break	Modules: Structure Theorem for Finitely Generated Modules over a PID	EXAM
Oct 22 – Oct 26 C1 & C2 DF: 10.4 L: 16.1–16.2	Tensor products	Tensor products: practice	Tensor products: maps, extension of scalars
Oct 29 – Nov 2 C1 & C2 DF: 11.5 L: 16.4–16.8	Tensor product: basic properties	Tensor product: more practice	Tensors in the wild
Nov 5 – Nov 9 L: 15.1–15.3 HK: 10.1 – 10.2	Higher tensors, symmetric and alternating maps	Bilinear forms	Symmetric bilinear forms
Nov 12 – Nov 16 L: 15.4 – 15.7 HK: 10.2	Inner products	Review day	The Snake Lemma
Nov 19 – Nov 23 DF: 10.5, 17.1 L: 16.3, 20.1–20.2	Homological algebra: introduction	Homological algebra: the long exact sequence	No Class – Thanksgiving Break
Nov 26 – Nov 30 DF: 17.1	Homological algebra: derived functors	Homological algebra: Ext and Tor	Homological algebra: flatness and extensions
Dec 3 – Dec 7 DF: 17	Homological algebra: Koszul complexes	Group cohomology: introduction	Group cohomology:the bar or standard resolution
Dec 10 – Dec 14	Semester recap	No class	No class

Please report any errors you find to smdbackr@umich.edu

Worksheet for 5 Sep 2018
Introduction: rings, modules, and algebras

Vocabulary: ring, commutative ring, zero ring, ring homomorphism, module, module homomorphism, unital, algebra, algebra homomorphism, endomorphism ring, units

The goal of this worksheet is to introduce the basic mathematical objects of Math 593. It is assumed that you have taken a good undergraduate abstract algebra course, so most of the underlying ideas should be (at least dimly) familiar to you.

Definition. A *ring* is a set R with two operations:

- $+\colon R \times R \to R$ (called *addition*) and
- $*\colon R \times R \to R$ (called *multiplication*)

satisfying the following axioms:

R1: $(R, +)$ is an abelian group,
R2: $*$ is associative: $r * (s * t) = (r * s) * t$ for all $r, s, t \in R$,
R3: multiplication is both left and right distributive with respect to addition: for all $r, s, t \in R$ we have $r * (s + t) = r * s + r * t$ (called *left-distributivity*) and $(s + t) * r = s * r + t * r$ (called *right-distributivity*), and
R4: there exists $1_R \in R$ for which $1_R * r = r * 1_R = r$ for all $r \in R$.

Warning: Not everyone assumes that their rings have a multiplicative identity element.[1]

We will almost always drop the symbol $*$ and write ab for $a * b$; similarly, we will write 1 for 1_R. A ring is said to be *commutative* provided that its multiplicative operation is commutative. A *zero ring* is a ring with one element.

(1) Show that $\mathbb{N}$ is not a ring. Show that $\mathbb{Z}$ is a ring.
(2) Suppose R is a ring. Show $\mathrm{Mat}_{n\times n}(R)$ is a ring with respect to matrix multiplication. When is it commutative?
(3) Suppose R is a ring. Show that R is a field if and only if (i) R is not a zero ring, (ii) R is commutative, and (iii) $R^\times = R \setminus \{0\}$. Here, $R^\times := \{r \in R\colon \text{ there exists } s \in R \text{ for which } rs = sr = 1\}$ is the group of *units* in R.

Definition. Suppose $(R, +_R, *_R, 1_R)$ and $(S, +_S, *_S, 1_S)$ are two rings. A function $f\colon R \to S$ is called a *ring homomorphism* provided that

- $f(a +_R b) = f(a) +_S f(b)$ for all $a, b \in R$,
- $f(a *_R b) = f(a) *_S f(b)$ for all $a, b \in R$, and
- $f(1_R) = 1_S$

The set of ring homomorphisms from R to S is denoted $\mathrm{Hom}(R, S)$ or $\mathrm{Hom}_{\mathrm{ring}}(R, S)$.

Caution. If H and G are groups, then the set of group homomorphisms from H to G is denoted $\mathrm{Hom}(H, G)$ or $\mathrm{Hom}_{\mathrm{grp}}(H, G)$. What an undecorated $\mathrm{Hom}(X, Y)$ means depends on context (see, for example, Prompt 11).

(4) Suppose R is a ring. Can you describe $\mathrm{Hom}(\mathbb{Z}, R)$?

Defintion. Suppose R is a ring. A *left R-module* is a set M with two operations:

- $+\colon M \times M \to M$ (called *addition*) and
- $*\colon R \times M \to M$ (called *scalar multiplication*)

satisfying the following axioms:

M1: $(M, +)$ is an abelian group,
M2: $(r + s) * m = r * m + s * m$ for all $r, s \in R$ and $m \in M$
M3: $(rs) * m = r * (s * m)$ for all $r, s \in R$ and $m \in M$
M4: $r * (m + n) = r * m + r * n$ for all $r \in R$ and $m, n \in M$

The map $*\colon R \times M \to M$ is called an *action* of R on M and the elements of R are often called *scalars*.

(5) Show that $\mathbb{Z}^2$ is a left-$\mathrm{Mat}_{2\times 2}(\mathbb{Z})$-module by having $X \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ act on $\mathbb{Z}^2$ by taking $v \in \mathbb{Z}^2$ to Xv.
(6) Formulate the definition of a right R-module (the scalar multiplication map will look like $M \times R \to M$). Show that $\mathbb{Z}^2$ is a right-$\mathrm{Mat}_{2\times 2}(\mathbb{Z})$-module by having $X \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ act on $\mathbb{Z}^2$ by taking $v \in \mathbb{Z}^2$ to $X^T v$.

Defintion. Suppose R is a ring. An R-module M is said to be *unital* provided that $1 * m = m$ for all $m \in M$.

[1] A ring with out an identity is sometimes referred to as a *rng*.

Please report any errors you find to smdbackr@umich.edu

Most modules you will encounter in the wild are unital; thus, following common convention, the phrase "M is an R-module" will **always** mean "M is a unital left R-module."

(7) Show that every $\mathbb{Z}$-module is an abelian group and every abelian group is a $\mathbb{Z}$-module.
(8) Suppose k is a field. Show that every k-module is a k-vector space and every k-vector space is a k-module.
(9) Suppose R is a commutative ring. Show that the polynomial ring $R[x_1, x_2, \ldots, x_n]$ is an R-module. Do we need to assume that R is commutative?

Definition. Suppose R is a ring and M and N are R-modules. A function $g\colon M \to N$ is called an *R-module homomorphism* provided that

- g is a group homomorphism and
- $g(rm) = rg(m)$ for all $r \in R$ and $m \in M$.

The set of R-module homomorphisms from M to N is denoted $\mathrm{Hom}_R(M, N)$ or $\mathrm{Hom}_{R-\mathrm{mod}}(M, N)$.

(10) Suppose R is a commutative ring and M is an R-module. Show $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ is an R-module. What if R is not commutative?
(11) Suppose R is a ring and M, N are R-modules. Must it be the case that $\mathrm{Hom}(M, N) = \mathrm{Hom}_R(M, N)$? [Hint: Consider complex conjugation.]

Defintion. Suppose R is a commutative ring. A set A is called an R-algebra provided that

- A is an R-module and
- there is an R-bilinear multiplication map $A \times A \to A$.

The notion of bilinearity arises quite often in Math 593, so understand it well. In the above definition it means $r * (a \cdot b) = (r * a) \cdot b = a \cdot (r * b)$, $a \cdot (b + c) = a \cdot b + a \cdot c$, and $(a + b) \cdot c = a \cdot c + b \cdot c$ for any $a, b, c \in A$ and $r \in R$. Here $*\colon R \times A \to A$ denotes the action of R on the R-module A and $\cdot\colon A \times A \to A$ is the multiplication map on the ring A. We will almost always drop the symbols $*$ and $\cdot$ and write $r(ab) = (ra)b = a(rb)$, $a(b+c) = ab+ac$, and $(a+b)c = ac+bc$.

(12) Suppose R is a ring and M is an R-module. Is $\mathrm{End}_R(M)$ an R-algebra? What if R is commutative?
(13) The set of symmetric real matrices with multiplication $(xy + yx)/2$ form an algebra. Show that multiplication is commutative, but not associative.
(14) As a real vector space Hamilton's quaternions, $\mathbb{H}$, have as a basis $(1, i, j, k)$; thus a *quaternion* is an expression of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$. We define multiplication on $\mathbb{H}$ by requiring (i) $rx = xr$ for every $x \in (1, i, j, k)$ and every $r \in \mathbb{R}$ and (ii) setting $i^2 = j^2 = k^2 = ijk = -1$.
  (a) Show that $ij = -ji = k$, $jk = -kj = i$, and $ik = -ki = -j$.
  (b) Show that multiplication is associative but not commutative.
  (c) Show that the center of $\mathbb{H}$ is $\mathbb{R} \simeq \mathbb{R}1$.
(15) Show that the cross product on $\mathbb{R}^3$ defines an $\mathbb{R}$-algebra that is neither associative nor commutative.

Definition. Suppose R is a commutative ring and A_1, A_2 are two R-algebras. A function $f\colon A_1 \to A_2$ is an *R-algebra homomorphism* provided that

- f is an R-module homomorphism and
- $f(ab) = f(a)f(b)$ for all $a, b \in A_1$.

The set of R-algebra homomorphisms from A_1 to A_2 is denoted $\mathrm{Hom}_{R-\mathrm{alg}}(A_1, A_2)$.

(16) Suppose R is a commutative ring and A is an R-algebra. What sort of object is $\mathrm{End}_{R-alg}(A) := \mathrm{Hom}_{R-alg}(A, A)$?

Something to Think About

Above we have defined both objects and morphisms for the categories[1] of rings, R-modules, and R-algebras. Based on these examples, what are some reasonable axioms that the objects and morphisms of a category should satisfy?

[1]The language of category theory will be freely used when it makes sense. There is no assumption that you have seen it before. See [A09, Chapter I §§3.1, 3.2, 4.1, 4.2] for a gentle introduction and the basic definitions.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 7 Sep 2018
Rings: products and Chinese Remainder Theorem

Vocabulary: Chinese Remainder Theorem, products, ideals, product ideal, comaximal, universal properties, isomorphism

Recall that if A and B are sets, then the product of A and B is the set $A \times B = \{(a, b) \mid a \in A, b \in B\}$. This can be extended to a product of any number of sets. If R and S are rings, then we want the product $R \times S$ to be more than just a set – we want it to be a ring. To make this happen we define addition and multiplication as follows

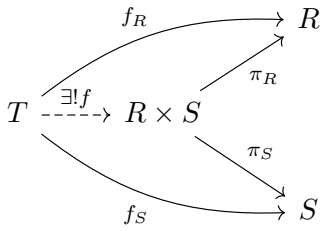
- $(r, s) + (r', s') = (r + r', s + s')$ for all $(r, s), (r', s') \in R \times S$ and
- $(r, s)(r', s') = (rr', ss')$ for all $(r, s), (r', s') \in R \times S$.

(17) Verify that axioms R1 through R4 hold for these operations.

(18) Show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ as rings.

The product operation is ubiquitous in mathematics, and we have just verified that products[1] can be defined both in the category of sets and the category of rings. How to characterize products, should they exist, in the category of groups or the category of modules or the category of algebras or . . . ? Universal properties are a handy tool for approaching this question.

Universal Property of Products in Rings. Suppose R and S are rings. The *product* of R and S is a ring, denoted $R \times S$, together with two ring homomorphisms $\pi_R \colon R \times S \to R$ and $\pi_S \colon R \times S \to S$ such that for every ring T and every pair of ring homomorphisms $f_R \colon T \to R$ and $f_S \colon T \to S$ there is a unique ring homomorphism $f \colon T \to R \times S$ for which the following diagram commutes.

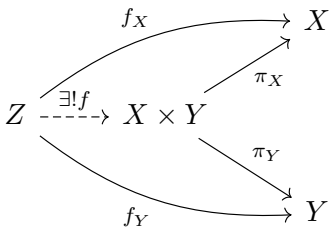


The maps π_R and π_S are usually called projections and f is often denoted as $f_R \times f_S$.

(19) Show that the product ring $R \times S$ (see Prompt 17), together with its natural projection maps, satisfies the universal property of products.

For a general category, the universal property of products looks like:

Universal Property of products. Suppose $\mathcal{C}$ is a category. For objects X and Y in $\mathcal{C}$, a product of X and Y is an object in $\mathcal{C}$, denoted $X \times Y$, together with a pair of morphisms $\pi_X \colon X \times Y \to X$ and $\pi_Y \colon X \times Y \to Y$ that satisfy the following universal property: for every object Z in $\mathcal{C}$ and pair of morphisms $f_X \colon Z \to X$, $f_Y \colon Z \to Y$ there exists a unique morphism $f \colon Z \to X \times Y$ such that the following diagram commutes:



Warning: products need not exist (consider the category of fields)! However, when they do exist, they are unique up to unique isomorphism[2]:

(20) Suppose Q is an object in $\mathcal{C}$ that, along with morphisms $\tilde{\pi}_X \colon Q \to X$ and $\tilde{\pi}_Y \colon Q \to Y$, satisfies the universal property of products. Show that there exists a unique isomorphism from Q to $X \times Y$. [Hint: Think about $\mathrm{Id}_{X \times Y}$ and use uniqueness.]

---

[1] Some people draw a distinction between an internal product and an external product. If $A, B \subset X$ and $A \times B \simeq X$, then one says that X is an internal product (of A and B); if A and B are not subobjects, then one says that the product is an external product. I have found that this language muddies the waters, especially for students; so I avoid it.

[2] For A, B in $\mathcal{C}$ we say $T \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an *isomorphism* provided there exists $S \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ for which $S \circ T = \mathrm{Id}_A$ and $T \circ S = \mathrm{Id}_B$.

Please report any errors you find to smdbackr@umich.edu

As an application of products, we now look at the Chinese Remainder Theorem. We need to introduce a few ideas.

Definition. Suppose R is a ring. A subset $I \subset R$ is called a *left ideal* provided that

I1: $(I, +)$ is a subgroup of $(R, +)$; and
I2: for all $r \in R$ we have $rI \subset I$, that is $rx \in I$ for all $x \in I$.

It is called a *right ideal* provided that

I1: $(I, +)$ is a subgroup of $(R, +)$; and
I2: for all $r \in R$ we have $Ir \subset I$, that is $yr \in I$ for all $y \in I$.

A subset of R that is both a left and right ideal is called an *ideal* or *two-sided ideal*.

If R is commutative, then every left ideal is a right ideal is a two-sided ideal is an ideal.

(21) Suppose R is a ring. Show that R and $\{0\}$ are always ideals of R.
(22) Show that if A and B are ideals, then $A + B$ is also an ideal.
(23) Show that $m\mathbb{Z}$ is an ideal in $\mathbb{Z}$ and $(x - 5)\mathbb{Q}[x]$ is an ideal in $\mathbb{Q}[x]$.
(24) Fix $n > 2$ and $1 \leq k \leq n$. Let I be the subset of $R = \mathrm{Mat}_{n\times n}(\mathbb{Q})$ consisting of matrices with nonzero entries only in the kth row. Is I a left ideal? Is it a right ideal? Can it be written as xR or Rx for a single $x \in I$?
(25) Suppose R and S are rings and $\varphi \in \mathrm{Hom}(R, S)$. Show that $\ker(\varphi)$ is an ideal of R. Is $\mathrm{im}(\varphi)$ an ideal of S?

Prompt 25 brings back memories of the first isomorphism theorem. Recall (or see Homework (26)) that for any ideal I of R we have that R/I, with the natural operations, is also a ring. It is called a quotient ring. Moreover, $R/\ker(\varphi) \simeq \mathrm{im}(\varphi)$.

While the notion of greatest common divisor doesn't make sense for a general commutative ring (why?), the notion of relatively prime does generalize:

Definition. Suppose R is a commutative nonzero ring. Ideals A, B of R are said to be *comaximal* provided that $A + B = R$. This means that there exist $a \in A$ and $b \in B$ so that $a + b = 1$.

(26) Suppose $n, m \in \mathbb{Z} \setminus \{0\}$. Show that $n\mathbb{Z}$ and $m\mathbb{Z}$ are comaximal if and only if $(n, m) = 1$.

Definition. Suppose R is a commutative nonzero ring. The *product* of ideals A and B in R is the ideal, denoted AB, consisting of all finite sums $\sum a_i b_i$ with $(a_i, b_i) \in A \times B$. The product of any finite number of ideals is defined similarly.

(27) Show that the ideal $n\mathbb{Z}m\mathbb{Z}$ is $n\mathbb{Z} \cap m\mathbb{Z}$ when $(m, n) = 1$. Generalize this result to a pair of ideals A and B in a nonzero commutative ring R. [Hint: use the word comaximal.] Is the converse of your general statement true?
(28) Suppose that R is a nonzero commutative ring. Suppose $I_1, I_2, I_3, \ldots, I_k$ are ideals in R that are pairwise comaximal. Show that the ideals I_1 and $I_2 I_3 \cdots I_k$ are comaximal. [Hint: consider $\prod_{j=2}^{k}(x_{1j} + x_j) \ldots$.]
(29) Suppose that R is a nonzero commutative ring. Suppose $I_1, I_2, I_3, \ldots, I_k$ are ideals in R that are pairwise comaximal. Show that $I_1 I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k$. [Hint: induction.]
(30) (Chinese Remainder Theorem[1]) Suppose R is a nonzero commutative ring. Let $I_1, I_2, \ldots, I_k$ be ideals and let

$$\varphi\colon R \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

denote the natural ring homomorphism. Show that the kernel of φ is $I_1 \cap I_2 \cap \cdots \cap I_k$. Show also that if $I_1, I_2, \ldots, I_k$ are pairwise comaximal, then the map is surjective and so

$$R/(I_1 I_2 \cdots I_k) \simeq R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

Something to Think About

The Lagrange Interpolation Theorem says that if $a_1, a_2, \ldots, a_k$ are distinct elements of a field F and $b_1, b_2, \ldots, b_k$ are elements of F, then there is a unique polynomial $p \in F[x]$ of degree less than k for which $p(a_i) = b_i$ for $1 \leq i \leq k$. The usual approach to proving this theorem is to use the Vandermonde[2] determinant. Since the statement "$p(a_i) = b_i$" is equivalent to the statement "$p(x) - b_i$ is zero in $F[x]/(x - a_i)F[x]$" can you use the Chinese Remainder Theorem to prove the Lagrange Interpolation Theorem? [Hint: Consider $p_i(x) = b_i(\prod_{j\neq i}(x - a_j))/(\prod_{j\neq i}(a_i - a_j)) \ldots$]

[1] "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?" – Sunzi Suanjing (3rd century)

[2] "[. . .] the name of Vandermonde would be ignored by the vast majority of mathematicians if it had not been attributed to the determinant that you know well, and which is not his!" –Henri Lebesgue

Please report any errors you find to smdbackr@umich.edu

Worksheet for 10 Sep 2018
Rings: quotients and localization

Vocabulary: multiplicative subset, localization, localization map, ring of fractions

Last time we saw how to create new rings from old ones by taking their product. Today we consider two additional ways to create new rings: localization and quotients. The construction of ring quotients is done in Homework (26).

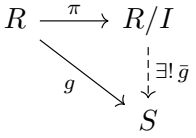
(31) What is R/R? What is $R/\{0\}$?

(32) If R is a commutative ring and $I \subset R$ is an ideal, then R/I is commutative. Is the converse true?

(33) Describe $\mathbb{R}[x]/(x^2+1)$.

Ring quotients are characterized by the following universal property:

Universal Property of ring quotients. Suppose R is a ring and $I \subset R$ is an ideal. A *quotient of R by I* is a ring, denoted R/I, together with a ring homomorphism $\pi\colon R \to R/I$ such that for every ring S and every ring homomorphism $g\colon R \to S$ for which $g(I) = 0$ there exists a unique ring homomorphism $\bar{g}\colon R/I \to S$ for which the following diagram commutes.



(34) Suppose R is a ring and $I \subset R$ is an ideal. Show that the quotient of R by I is unique up to unique isomorphism.

We now resume our study of localization that we began in Homework (2).

Definition. Suppose R is a commutative ring and $D \subset R$. We say D is a *multiplicative subset of R* if $1 \in D$ and D is closed under multiplication, i.e., if $s, t \in D$ then $st \in D$.

(35) Suppose p is a prime. Is $\mathbb{Z} \setminus p\mathbb{Z}$ a multiplicative subset of $\mathbb{Z}$?

You should associate the letter D with the word "denominator." Given a commutative ring R and a multiplicative subset D of R, we define a relation on $R \times D$ by declaring $(r, d) \sim (s, e)$ provided that there exists $f \in D$ such that $(re - sd)f = 0$.

(36) Verify that this defines an equivalence relation on $R \times D$.

Let r/d denote the equivalence class of $(r, d) \in R \times D$ and let $D^{-1}R$ denote the set of all equivalence classes. Define addition and multiplication in $D^{-1}R$ as follows:

$$r/d + s/e = (re + sd)/de, \quad r/d \cdot s/e = rs/de$$

(37) Verify that these operations define a ring structure on $D^{-1}R$.

Definition. Suppose R is a commutative ring and $D \subset R$ is multiplicative. The ring $D^{-1}R$ is called the *localization of R with respect to D* or *ring of fractions of R with respect to D*

(38) Examples.

(a) Let $D = \mathbb{Z} \setminus \{0\} \subset \mathbb{Z}$. What is $D^{-1}\mathbb{Z}$?

(b) Suppose k is a field and $D \subset k$ is multiplicative. What is $D^{-1}k$?

(c) Suppose $a, b \in \mathbb{Z}_{>1}$ and $(a, b) = 1$. Let $R = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ and take $D = \{(1, 1), (0, 1)\}$ What is $D^{-1}R$?

(d) Suppose R is a commutative ring and $f \in R$. Let $D = \{f^n \mid n \in \mathbb{Z}_{\geq 0}\}$ and set $R_f = D^{-1}R$. Show that R_f is the zero ring if and only if f is nilpotent (i.e., $f^m = 0$ for some $m \in \mathbb{N}$).

(e) Fix a prime p and let $D = \mathbb{Z} \setminus p\mathbb{Z}$. The ring $\mathbb{Z}_{(p)} := D^{-1}\mathbb{Z}$, called the localization of the integers at p, is very important in number theory. Find an infinite number of distinct ideals in $D^{-1}\mathbb{Z}$. Is your list exhaustive?

(f) Describe $\mathbb{C}[x]_x$.

(39) Show that $D^{-1}R$ is the zero ring if and only if $0 \in D$.

(40) Define a map $\ell\colon R \to D^{-1}R$ by $\ell(r) = r/1$. The map ℓ is often called the *localization map*.

(a) Show that ℓ is a ring homomorphism.

(b) Let $R = \mathbb{Q}[x, y]/(xy)$ and suppose D is the set of powers of x. Is the localization map $R \to R_x = D^{-1}R$ injective?

(c) Verify that if D contains no zero divisors[1], then the localization map ℓ is injective.

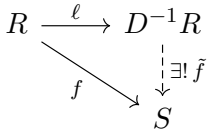
(41) Suppose R and S are commutative rings and $D \subset R$ is multiplicative. Suppose $f \in \mathrm{Hom}(R,S)$ with $f(D) \subset S^\times$.

(a) Show that there is a R-map $\tilde{f}\colon D^{-1}R \to S$ for which $\tilde{f} \circ \ell = f$. Here ℓ is the localization map.

(b) Show that $\tilde{f}$ is the unique such map.

This suggests that localization can be characterized in terms of a universal property, and indeed:

Universal Property of localization. Suppose R is a commutative ring and $D \subset R$ is multiplicative. A *localization of R with respect to D* is a ring, denoted $D^{-1}R$, together with a ring homomorphism $\ell\colon R \to D^{-1}R$ such that for every commutative ring S and every $f \in \mathrm{Hom}(R,S)$ with $f(D) \subset S^\times$ there exists a unique ring homomorphism $\tilde{f} \in \mathrm{Hom}(D^{-1}R, S)$ for which the following diagram commutes.



(42) Show that a localization of R with respect to D is unique up to unique isomorphism.

Something to Think About

The map $|\ |_p : \mathbb{Z}_{(p)} \to \mathbb{R}$ defined by

$$|x|_p = \begin{cases} p^{-n} & \text{if } x \in p^n\mathbb{Z}_{(p)} \setminus p^{n+1}\mathbb{Z}_{(p)} \\ 0 & \text{otherwise} \end{cases}$$

is multiplicative and satisfies $|x+y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$. Thus, $\mathrm{dist}(a,b) = |a-b|_p$ defines a metric on $\mathbb{Z}_{(p)}$. The metric space completion of $\mathbb{Z}_{(p)}$ is denoted $\mathbb{Z}_p$ and called the *p-adic integers*. The principal ideal $p\mathbb{Z}_p$ is the maximal ideal in $\mathbb{Z}_p$, and $\mathbb{Z}_p/p\mathbb{Z}_p$ is a finite field with p elelments. The localization of $\mathbb{Z}_p$ with respect to $\mathbb{Z}_p \setminus \{0\}$ is $\mathbb{Q}_p$, the *field of p-adic numbers*. The norm $|\ |_p$ extends (uniquely) to a norm on $\mathbb{Q}_p$, and $\mathbb{Z}_p$ may be identified with $\{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. With respect to this norm the field $\mathbb{Q}_p$ is a locally compact field of characteristic zero. $\mathbb{R}$ and $\mathbb{C}$ are also locally compact fields of characteristic zero, might there be others?

[1]For a general ring R and $a \in R$ we say that a is a zero divisor provided that either of the maps $r \mapsto ar$ or $r \mapsto ra$ from R to R is not injective.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 12 Sep 2018
Rings: UFDs and Noetherian rings

Vocabulary: domain, integrable domain, irreducible element, principal ideal, prime ideal, maximal ideal, prime element, Unique Factorization Domain, UFD,

The purpose of this worksheet is to introduce Unique Factorization Domains; this requires the introduction of a considerable amount of vocabulary.

Definition. Suppose R is a ring and $I \subset R$ is an ideal. I is called *principal* provided that $I = (r)$ for some $r \in R$.

(43) Show that every ideal in $\mathbb{Z}$ is principal.
(44) Suppose R is a commutative ring. Show that for all $a, b \in R$ we have $(ab) = (a)(b)$.

Definition. Suppose R is a ring and $I \subsetneq R$ is an ideal. I is said to be a *prime ideal* provided that if the product ideal AB is contained in I, then $A \subset I$ or $B \subset I$.

(45) Suppose R is commutative. Show that a proper ideal I in R is prime if and only if whenever $ab \in I$ with $a, b \in R$ then at least one of a or b is an element of I. When R is commutative it is also true that I is prime iff R/I has no zero divisors (see Homework (47)).
(46) What are the prime ideals in $\mathbb{Z}$?
(47) Show that the ideal $(5, x)$ in $\mathbb{Z}[x]$ is prime but not principal.

Definition. Suppose R is a ring and $I \subsetneq R$ is an ideal. I is said to be a *maximal ideal* provided that whenever $J \subset R$ is an ideal and $I \subsetneq J$ we have $J = R$.

Thanks to the Kuratowski-Zorn[1] lemma, maximal ideals exist (see [DF04, Proposition 11, p. 254]).

(48) Does $\mathbb{Z}$ have any prime ideals which are not maximal?
(49) Show that the ideal (x) in $\mathbb{Z}[x]$ is prime but not maximal.

It is difficult to say interesting things about a general ring, even an arbitrary commutative ring. We now begin the process of narrowing the class of rings we will consider – the proliferation of names (Euclidean, UFD, PID, ...) can be a bit overwhelming, so I recommend creating a scorecard.[2]

Definition. A ring R is called a *domain* provided that R is nonzero and for all $a, b \in R$ we have $ab = 0$ implies $a = 0$ or $b = 0$. A commutative domain is called an *integral domain*.

Hamilton's quaternions $\mathbb{H}$ (see Prompt 14) provide an example of a domain which is not an integral domain.

(50) When is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?
(51) Suppose k is a field. Is k an integral domain? Is $k[x, y]$ an integral domain? Is $\mathrm{Mat}_{m\times m}(k)$ a domain?

Definition. Suppose R is a commutative ring and r is a nonzero element of $R \setminus R^\times$. The element r is called *irreducible* provided that whenever $r = ab$ with $a, b \in R$, then at least one of a or b is a unit in R. The element r is called *prime* provided that (r) is a prime ideal (that is, whenever $r \mid ab$ for $a, b \in R$ we have $r \mid a$ or $r \mid b$). The element r is called *composite* provided that it can be written as the product of two non-units.

In general, the notions of irreducible and prime are not strongly correlated. However, as we will see, (a) every prime element in an integral domain is irreducible and (b) the two notions are equivalent in UFDs.

(52) Suppose $R = \mathbb{Z}/10\mathbb{Z}$. Show that 5 is prime but not irreducible.
(53) Consider the ring $\mathbb{Z}[\sqrt{-13}]$.
  (a) Show that if $7 = (a+b\sqrt{-13})(c+d\sqrt{-13})$, then one of $(a+b\sqrt{-13})$ or $(c+d\sqrt{-13})$ is a unit in $\mathbb{Z}[\sqrt{-13}]$. [Hint: Use the norm map.] Conclude that 7 is irreducible.
  (b) Note that $(6+\sqrt{-13})(6-\sqrt{-13}) = 7^2$. Conclude that 7 is not prime in $\mathbb{Z}[\sqrt{-13}]$.

[1] The sculptures between Randall and West are by Jens Zorn, son of Max Zorn for whom the Kuratowski-Zorn lemma is half-named.
[2] "The only way anyone can keep track of all the different types of rings is to have specific examples for each adjective." –Charlotte Chan

$\mathbb{Z}[\sqrt{-13}]$ is an example of a quadratic integer ring. Quadratic fields[1] and their rings of integers are a good source of illustrative examples in the study of algebra and algebraic number theory.[2]

(54) What are the irreducible elements of $\mathbb{Z}$?

(55) Suppose R is an integral domain. Show that if $r \in R$ is prime, then it is irreducible.

Definition. A *Unique Factorization Domain* or *UFD* is an integral domain R is which every nonzero $r \in R \setminus R^\times$ has the following properties:

- (factorization) r can be written as a finite product of (not necessarily distinct) irreducibles p_i of R: $r = p_1 p_2 \cdots p_n$.
- (uniqueness of factorization) if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles then $m = n$ and there exists $\sigma \in S_n$ so that $p_j \in q_{\sigma(j)} R^\times$ for $1 \leq j \leq n$.

In plain language, in a UFD every non-zero non-unit can be written uniquely (up to reordering and unit multiple) as a product of irreducible elements. Thanks to the Fundamental Theorem of Arithmetic (which relies on Euclid's Lemma: if $p \mid ab$, then $p \mid a$ or $p \mid b$) we know $\mathbb{Z}$ is a UFD.

(56) Show that $\mathbb{Z}[\sqrt{-13}]$ is not a UFD. [Hint: look at the number fourteen and Homework (71).]

Since the word "uniqueness" appears in its name, it is natural to ask how generally one can expect non-zero non-units to factorize into irreducibles (regardless of uniqueness). The answer is: quite generally.

Definition. A ring R is called *Noetherian*[a] provided that it satisfies the ascending chain condition for left ideals. That is, R has no infinite increasing chains of left ideals.

[a] Named for the great 20th century mathematician Emmy Noether

We should call such a ring *left-Noetherian*, but we won't. By the way, the Data Base of Ring Theory[3] can be a useful tool. For example, a search for a ring that is left-Noetherian but not right-Noetherian returns a number of examples.

(57) Suppose R is a Noetherian integral domain. Let $r \in R \setminus R^\times$ be nonzero. We wish to establish that r can be written as a product of a finite number of irreducible elements of R.

(a) If r is irreducible, then we are done.

(b) Suppose r is not irreducible, then $r = r_1 r_2$ for some $r_1, r_2 \in R \setminus R^\times$ (why?). If r_1 and r_2 are irreducible, then we are done. If not, at least one, let's say r_1 is reducible. Show that $(r) \subsetneq (r_1) \subsetneq R$.

(c) Since r_1 is not irreducible, then $r_1 = r_{11} r_{12}$ for some $r_{11}, r_{12} \in R \setminus R^\times$ (why?). If r_{11} and r_{12} are irreducible, then we are done with r_1. If not, at least one, let's say r_{11} is reducible. Show that $(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq R$.

(d) Show that r factors into a finite number of irreducible elements of R.

Something to Think About

Noetherian rings play a central role in both commutative and non-commutative algebra; what properties do they have? For example: If R is Noetherian and $I \subset R$ is an ideal, is R/I Noetherian? is I Noetherian? is $R[x]$ Noetherian? is $R[x_1, x_2, \ldots, x_n]$ Noetherian? Is a subring[4] of R also Noetherian? Is the localization of R also Noetherian?

Warning: Not every UFD is a Noetherian ring. UFDs satisfy a weaker condition: the ascending chain condition for principal ideals. Note that the proof in Prompt 57 uses this weaker condition. As one might expect, there are rings that satisfy the ascending chain condition for principal ideals, yet are not UFDs.

[1] A field k is called a *quadratic field* provided that $\mathbb{Q} \subset k$ and k is a two dimensional $\mathbb{Q}$-vector space. For example, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, or $\mathbb{Q}[\sqrt{-13}]$. The description of the corresponding quadratic integer ring, usually denoted $\mathcal{O}_k$, can appear mysterious and non-uniform (see, for example, [DF04, §7.1, p. 229]). The mystery disappears when one learns that $\mathcal{O}_k$ is, by definition, the ring of elements of k that satisfy a monic polynomial in $\mathbb{Z}[x]$.

[2] See, for example, Milne's notes on algebraic number theory at http://www.jmilne.org/math/CourseNotes/.

[3] ringtheory.herokuapp.com/

[4] A *subring* of R is a subset of R that is a ring with respect to the inherited addition and multiplication operations. Some people assume that the identity of the subring is the identity of R; we do not.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 14 Sep 2018
Rings: PIDs and Euclidean domains

Vocabulary: Principal Ideal Domain, PID, norm, positive norm, Euclidean Domain,

Definition. A *Principal Ideal Domain* or *PID* is an integral domain in which every ideal is principal.

The integers are a PID, and we shall soon learn that for a field k the ring $k[x]$ is also a PID. If $D \in \mathbb{Z}_{<0}$ is square free, then[1] the quadratic ring of integers $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$ is a PID if and only if $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. The set of positive square free D for which $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$ is a PID is not known – in fact, we don't know if it is a finite set or not.

(58) Suppose R is a PID. Show that every nonzero prime ideal in R is a maximal ideal. [Hint: Let (m) be an ideal between (p) and R.]

(59) Suppose R is a PID and $r \in R$ is irreducible. Show that (r) is a maximal ideal in R. [Hint: Argue by contradiction.] Conclude that an element of a PID is irreducible if and only if it is prime. [Hint: Homework 47.]

We have the tools to show that every PID is a UFD.

(60) Show that every PID is Noetherian. [Hint: If $I_1 \subset I_2 \subset \dots$ are ideals in a ring R, then so too is $\cup I_j$.] Conclude that every non-zero non-unit in a PID has a factorization into prime elements. (why prime?)

(61) Show that the factorization created in Prompt 60 is unique (up to units). Suppose $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ where the p_j (resp. q_k) are not necessarily distinct primes. We need to show that $n = m$ and there is some $\sigma \in S_n$ for which $p_i \in q_{\sigma(i)} R^\times$ for $1 \le i \le n$.
We first handle the case $n = 0$. In this case, r is a unit. If $m \neq 0$, then r has some other factorization as qs with q irreducible and $s \in R$. But then $q \mid r$ and so by Homework 19 we conclude that $q \in R^\times$, contradiction. Suppose now that $n \ge 1$, and proceed by induction:
   (a) Show that, WOLOG, $p_1 \mid q_1$. Conclude that $q_1 = p_1 u$ with u a unit in R. Cancel p_1 from both sides to obtain $1 = (uq_2)q_3 \cdots q_m$. Apply Homework 19 to conclude that $m = 1$.
   (b) Suppose $n \ge 1$. As above, WOLOG $p_1 \mid q_1$ and $q_1 = p_1 u$ with u a unit in R. Cancel to obtain $p_2 p_3 \cdots p_n = (uq_2)q_3 \cdots q_m$. Apply induction.

(62) Conclude that every PID is a UFD.

Another important class of integral domains are those that possess a division algorithm. These rings are often called Euclidean domains.

Definition. Suppose R is an integral domain. A *norm* on R is any function $N \colon R \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. The function N is said to be a *positive norm* provided that $N(r) > 0$ for all nonzero r.

The normal absolute value on $\mathbb{Z}$ yields a positive norm. If k is a field, then $p \mapsto \deg(p)$ on $k[x]$ yields a norm.[2] The norm map $N(a + bi) = a^2 + b^2$ on the Gaussian Integers $\mathbb{Z}[i]$ is a positive norm.

Definition. An integral domain R is called an *Euclidean Domain* provided that there is a positive norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ with

$$a = bq + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

The element q is called the quotient and the element r is called the remainder of the division.

Important examples of Euclidean Domains include $\mathbb{Z}$, the localization of $\mathbb{Z}$ at a prime, and $k[x]$ for k a field. If $D \in \mathbb{Z}_{<0}$ is square free, then the quadratic ring of integers $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$ is a Euclidean Domain if and only if $D \in \{-1, -2, -3, -7, -11\}$; thus, not every PID is a Euclidean Domain (see [DF04, Exercise 8, p. 278]).

(63) Show that q and r need not be unique by considering $a = 3 + 5i$ and $b = 2$ in $\mathbb{Z}[i]$.

Since we have claimed that $k[x]$ is a PID when k is a field, it would be excellent if every Euclidean Domain was a PID. This is the content of the next prompt.

(64) Suppose R is a Euclidean Domain with an associated (positive) norm map $N \colon R \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. Let $I \subset R$ be an ideal. We wish to show that I is a principal ideal. If $I = \{0\}$, then we are done. So, suppose I is nonzero.
   (a) Show there exists $0 \neq d \in I$ for which $N(d) \le N(s)$ for all nonzero $s \in I$.

[1] This is a nontrivial result.

[2] For many of us, the degree of the 0 polynomial is $-\infty$. This is why, unlike [DF04], we have defined norm functions on the nonzero elements only.

(b) Show that $I \subset (d)$. [Hint: Use the definition of Euclidean Domain!]

(c) Conclude R is a PID.

(65) (*Bonus*.) Suppose R is an integral domain. Is it possible for R to be a Euclidean Domain with respect to two different norm maps?

Something to Think About

In the literature, a norm map is often also required to be submultiplicative: $N(ab) \leq N(a)N(b)$ for all nonzero a, b. It is difficult to think of a Euclidean Domain for which the associated norm map doesn't have this property, but they do exist. However, if R is a Euclidean Domain with associated norm map d, then the function $N\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ defined by $N(c) = \min_{x \in R\setminus\{0\}} d(xc)$ is also a norm map with respect to which R is a Euclidean Domain, and it satisfies $N(ab) \leq N(a)N(b)$. (Do you see why?) An advantage of this approach is that the submultiplicativy of N is related to the factorization of non-zero non-units of R into irreducibles. Can you use this idea to show directly that every Euclidean Domain is a UFD?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 17 Sep 2018
Polynomials: Gauss' lemma and reducing polynomials mod I

Vocabulary: Gauss' Lemma, field of fractions, greatest common divisor, gcd

Suppose that R is a commutative ring. Determining whether or not a given polynomial in $R[x]$ is irreducible is an important and challenging problem that arises in nearly every branch of mathematics. Sometimes it is easy to address this problem – e.g., thanks to the Fundamental Theorem of Algebra[1] we know that the only irreducible nonconstant polynomials in $\mathbb{C}[x]$ are the linear ones. For a general ring (or even field) the problem is much more demanding; many approaches to the problem involve either "shrinking" the ring of coefficients by reducing the coefficients modulo some ideal in R or "enlarging" the ring of coefficients via localization.

Suppose $I \subset R$ is an ideal. We denote by (I) or $I[x]$ the ideal in $R[x]$ generated by I. There is a natural map from $R[x]$ to $(R/I)[x]$ that takes a polynomial $a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$ to the polynomial $\bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$ where $\bar{r}$ denotes the image of $r \in R$ in R/I. As is readily verified, the kernel of this map is $I[x]$ and so we have

$$(R/I)[x] \simeq R[x]/I[x].$$

(66) Show that if I is a prime ideal in R, then $I[x]$ is a prime ideal in $R[x]$. [Hint: Homework 47 may be helpful.]

(67) Suppose $q \in \mathbb{Z}[x]$ has degree greater than one. Show that there is a prime p so that the image of q in $(\mathbb{Z}/(p))[x]$ factors into two nonconstant polynomials of degree less than $\deg(q)$. [Hint: Don't think too hard and look at a nonunit in $q(\mathbb{Z})$.]

The polynomial $q(x) = x^2 - 2$ is irreducible in $\mathbb{Z}[x]$ (why?). Thanks to Prompt 67 there are many primes for which the image of q in $(\mathbb{Z}/(p))[x]$ factors. On the other hand, there are also many primes (e.g., 3, 5, 11, ...) for which the image of q in $(\mathbb{Z}/(p))[x]$ doesn't factor. As it turns out (see Prompt 77), the latter observation can be turned into a useful criterion for irreducibility: Suppose q is monic and nonconstant in $R[x]$; if we can find an ideal $I \subset R$ for which the image of q in $(R/I)[x]$ is irreducible, then q is irreducible in $R[x]$.

(Un)fortunately, looking at quotients does not provide a full solution: there exist irreducible monic polynomials q of degree greater than one in $\mathbb{Z}[x]$ for which the image of q in $(\mathbb{Z}/(p))[x]$ factors into two nonconstant polynomials of degree less than $\deg(q)$ for *every* prime p. Examples include the so-called Leibniz[2] polynomial $x^4 + 1$ (see [DF04, Corollary 16, p. 586]) and the qual[3] favorite $x^4 - 10x^2 + 1$ (see Homework 76).

Localization is another useful tool for studying questions of irreduciblity.

Definition. Suppose R is an integral domain. The *field of fractions* of R is the localization of R with respect to $R \setminus \{0\}$.

In Homework (52) you show that the field of fractions, F, of an integral domain R is, in fact, a field.

(68) What is the field of fractions of $\mathbb{Z}$?

(69) If $q \in R[x]$ is irreducible in $F[x]$ is it irreducible in $R[x]$?

We know that $R[x]$ is an integral domain. We also know that $F[x]$ is a Euclidean Domain, hence a PID (Prompt 64c), hence a UFD (Prompt 62). Thus, if $p \in R[x]$, then p factors uniquely in $F[x]$. Unfortunately, it does not follow that p factors[4] in $R[x]$.

(70) Let $R = \mathbb{Z}[2\sqrt{2}]$ and look at the polynomial $q(x) = x^2 - 2$. Show that q factors over the field of fractions of R, but is irreducible in $R[x]$.

To use localization to make statements about irreduciblity, we will need to place some restrictions on R. It turns out that $R[x]$ is a UFD if and only if R is a UFD (see Prompt 76), so we are going to concentrate on the case when R is a UFD.

(71) Suppose R is a UFD with field of fractions F. Let $p \in R[x]$. Suppose p factors as AB with $A, B \in F[x]$.
- (a) Show that we may clear denominators. That is, we may choose $r \in R$ and $s \in R$ so that $a' = rA$ and $b' = sB$ belong to $R[x]$. Let $t = rs$. We have $tp = a'b'$ in $R[x]$.
- (b) Show: If $t \in R^\times$, then p factors in $R[x]$.
- (c) If $t \notin R^\times$, then we can (uniquely) write $t = p_1p_2 \cdots p_m$ with p_i irreducible. Look at tp in $(R/(p_1))[x]$ and show that p_1 divides one of a' or b'. Conclude that we may cancel p_1 from tp and one of a' or b' and still have an equality in $R[x]$.

---

[1] If you have never seen a proof of this result, please let me know and we'll remedy that.

[2] So named because Leibniz mistakenly believed that it and its cousins $x^4 + a^2$ could not be factored over $\mathbb{R}$.

[3] It is a favorite because its roots are all four possibilties of $\pm\sqrt{2} \pm \sqrt{3}$; remember this when you take up Galois theory.

[4] Much less factors uniquely.

(d) (Gauss' Lemma) Conclude that we may factor p as ab with $a, b \in R[x]$.

Warning! a and b will not, in general, be A and B. For example, $x^2 - 1 = (6x/10 - 6/10)(5x/3 + 5/3)$ in $\mathbb{Q}[x]$. In this case we can take $t = 30 = (2)(5)(3)$ and $x^2 - 1 = (x-1)(x+1)$ in $\mathbb{Z}[x]$.

Suppose R is a UFD. Since every non-zero element of R is a unit in F, the field of fractions of R, it is too much to hope that an element of $R[x]$ is irreducible if and only if it is irreducible in $F[x]$ (go back and check your answer to Prompt (69)). However, after making some straightforward modifications, we can arrive at a characterization of the interesting irreducible elements in $R[x]$ in terms of those in $F[x]$.

Definition. Suppose A is a commutative ring and $a_1, a_2, \ldots a_m \in A$ not all zero. A *greatest common divisor* or *gcd* of $a_1, a_2, \ldots a_m$ is a nonzero $a \in A$ for which

- $a \mid a_j$ for $1 \leq j \leq m$ and
- if $a' \in A$ and $a' \mid a_j$ for $1 \leq j \leq m$ then $a' \mid a$.

(72) Suppose that A is a commutative ring and a is a gcd of $a_1, a_2, \ldots a_m \in A$ (not all zero). Show that (a) is the smallest principal ideal containing $a_1, a_2, \ldots a_m$.

(73) Suppose that A is an integral domain. Show that if $a, a' \in A$ with $(a) = (a')$, then there is a unit $u \in A^\times$ for which $a = ua'$. Conclude that the gcd of $a_1, a_2, \ldots, a_m \in A$ (not all zero) is unique up to units.

(74) Suppose R is a UFD and $p \in R[x]$ has the property that the gcd of its nonnzero coefficients is one.[1] Show that p is irreducible in $R[x]$ if and only if p is irreducible in $F[x]$.

(75) Suppose R is a UFD and $p \in R[x]$ is a monic polynomial. Show that p is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

We now have the tools to prove:

(76) R is a UFD if and only if $R[x]$ is a UFD. The direction from right to left is straightforward (look at the constant polynomials and don't think too hard), so we work on going from left to right. Suppose R is a UFD and let F denote its field of fractions. Suppose $q \in R[x]$.

(a) By considering the gcd of the coefficients of q, show that WOLOG we may assume that (a) the gcd of the coefficients of q is one and (b) $\deg(q) \geq 1$.

(b) Use Gauss' Lemma and Homework (64) to show that q factors as a product $q_1 q_2 \cdots q_m$ where (a) each $q_i \in R[x]$ is irreducible in $F[x]$ and (b) the gcd of the coefficients of q_j is one for $1 \leq j \leq m$.

(c) (Existence) Use Prompt (74) to conclude that q can be written as a finite product of irreducibles in $R[x]$.

(d) (Uniqueness). Suppose that we have two factorizations $p = q_1 q_2 \cdots q_m = q_1' q_2' \cdots q_n'$.

(i) Use Homework (64) and Prompt (74) to conclude that $p = q_1' q_2' \cdots q_n'$ is a factorization of p into irreducibles in $F[x]$. Conclude that $n = m$ and, WOLOG, $b_j q_j = a_j q_j'$ for some $a_j, b_j \in R^\times$.

(ii) Show that for each j there exists $u_j \in R^\times$ for which $a_j = u_j b_j$ and conclude that $q_j = u_j q_j'$, completing the proof of uniqueness.

Something to Think About

In Math 594 you will spend some time looking at the cyclotomic polynoimals Φ_n. One definition[2] of Φ_n is that it is the unique irreducible monic polynomial in $\mathbb{Z}[x]$ that divides $x^n - 1$ but not $x^m - 1$ for $m < n$. For a prime p, the cyclotomic polynomial Φ_p has the form

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

How to show this is irreducible in $\mathbb{Z}[x]$? Has anything we've done so far been useful for approaching this question?

[1] Such a polynomial is often called *primitive*. However, this term describes so many things in mathematics that it is best to not use it here.

[2] And, I think, the only one we can state with the words we know. It is nontrivial to show that there exists a polynomial that satisfies this definition.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 19 Sep 2018
Polynomials: irreducibility

Vocabulary: Schönemann–Eisenstein Criterion

In practice, it can be challenging to figure out when a given polynomial is irreducible. But there are some common and useful techniques; we discuss two of them here.

(77) Suppose R is a ring and I is a proper ideal in R. If $q \in R[x]$ is a nonconstant monic polynomial whose image in $(R/I)[x]$ cannot be factored into polynomials of smaller degree, then q is irreducible in $R[x]$.[Hint: Suppose q factors in $R[x]$.]

Since $R[x,y] \simeq (R[x])[y]$ and so on, this result also applies to polynomial rings in more than one variable.

(78) Are the following irreducible in $\mathbb{Z}[x]$?
  (a) $x^2 + x + 1$
  (b) $x^3 + 2x + 1$

(79) Are the following irreducible in $\mathbb{Z}[y,x]$?
  (a) $x^2 + xy + y^2 + 1$
  (b) $xy + x + y + 1$

(80) Is $xyz^2 + z + zx^3y + x^2 + 5x^2yz + xy + y^2 + 1 + xyz$ irreducible in $\mathbb{Z}[x,y,z]$?

The behavior of irreduciblity under composition is a subtle issue, but there is one case that is easy to handle.

(81) Suppose R is an integral domain and $f \in R[x]$. Define $\ell \in R[x]$ by $\ell(x) = mx + b$ where $m \in R^\times$ and $b \in R$. Show that f factors in $R[x]$ if and only if $f \circ \ell$ factors in $R[x]$.

The map $T \in \mathrm{Hom}(R[x], R[x])$ given by $T(f) = f \circ \ell$ is an example of a ring automorphism.

(82) (Schönemann–Eisenstein Criterion) Suppose R is an integral domain and $p \in R$ is prime. Suppose $q \in R[x]$ is a monic nonconstant polynomial of degree m with $q(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$. Show that if
- $p^2 \nmid a_0$ and
- $p \mid a_j$ for $0 \leq j < m$

then q is irreducible. [Hint: Use Prompt 77.]

(83) Suppose p is a prime. Show that the pth cyclotomic polynomial $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible. [Hint: Use Prompts (81) and (82).]

(84) Show that the following polynomials are irreducible in $\mathbb{Z}[x,y,z]$.
  (a) $x^3 - y^2x^2z^2 + 3xyz^2 + y^5z$
  (b) $x^3 + 4xy + 27x + 8y + 12$
  (c) $x^5 - y^3z + y^3 + 16x^2 + x^2yz^{27} + 47x + xyz - 13z^{78}x^4 + 739$

Something to Think About

Is the composition of irreducible polynomials irreducible? This is true over $\mathbb{C}$ (why?), but clearly not true over $\mathbb{R}$ (why not?). Note that in both cases, the degree of the irreducible components of the composition is divisible by the degree of the "outer polynomial." Could this be a general fact? Perhaps it is better to ask existence type questions. For example, given a nonconstant irreducible polynomial $p \in \mathbb{Q}[x]$, does there always exist a polynomial $q \in \mathbb{Q}[x]$ of degree at least 2 such that the composition $p \circ q$ is irreducible in $\mathbb{Q}[x]$?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 21 Sep
Modules: the fundamentals

Vocabulary: module, submodule, module homomorphism, companion matrix

We are now done with the "ring portion" of the course, and we are ready to start the "module portion." Recall that the phrase "M is an R-module" **always** means "M is a unital left R-module." That is:

Defintion. Suppose R is a ring. An *R-module* is a set M with two operations:

- $+\colon M \times M \to M$ (called *addition*) and
- $*\colon R \times M \to M$ (called *scalar multiplication*)

satisfying the following axioms:

M1: $(M, +)$ is an abelian group,
M2: $(r + s) * m = r * m + s * m$ for all $r, s \in R$ and $m \in M$
M3: $(rs) * m = r * (s * m)$ for all $r, s \in R$ and $m \in M$
M4: $r * (m + n) = r * m + r * n$ for all $r \in R$ and $m, n \in M$
M5: $1 * m = m$ for all $m \in M$.

Modules are everywhere. For example, $L^p([0,1])$ (but not $C^p([0,1])$) is a module over the ring $C^0([0,1])$ and the smooth differentiable p-forms (or vector fields or tensor fields) on a smooth manifold M are a module over the ring $C^\infty(M)$.

(85) Show that if R is the zero ring and M is an R-module, then $M = \{0\}$.
(86) Show that every $\mathbb{Z}$-module is an abelian group and every abelian group is a $\mathbb{Z}$-module. [Hint: If A is an abelian group, how should we define $n \cdot a$ for $n \in \mathbb{Z}$ and $a \in A$?]
(87) Suppose k is a field. Show that every k-module is k-vector space and every k-vector space is a k-module. [**Warning:** Thinking of modules as vector spaces is dangerous, wrong, and will lead you astray eventually; fields are just too special. It is, of course, OK to think of vector spaces as modules over a field.]
(88) Suppose V is a k-vector space. Show that V is an $\mathrm{End}_k(V) := \mathrm{Hom}_k(V, V)$ module in a natural way.
(89) Suppose R is a ring. Show that R^n is a module. If $I \subset R$ is an ideal, is R/I an R-module?

We know that abelian groups have subgroups and vector spaces have subspaces. In general, modules have submodules.

Definition. Let R be a ring and let M be an R-module. An *R-submodule* of M is a subgroup N of M which is closed under scalar multiplication, that is, $rn \in N$ for all $r \in R$ and $n \in N$.

(90) Show that every $\mathbb{Z}$-submodule of a $\mathbb{Z}$-module A is a subgroup of A.
(91) Suppose k is a field. Show that every k-submodule of a k-module V is a subspace of V.
(92) Suppose R is a ring and M is an R-module. Show that $N \subset M$ is a submodule of M if and only
- $N \neq \emptyset$ and
- $x + ry \in N$ for all $r \in R$ and $x, y \in N$.

(93) Suppose R is a ring. What are the R-submodules of R?

The following exercises go through an important example that will allow us to reformulate many linear algebra results as results about modules. Suppose k is a field and V is a k-vector space. We already know that V is a k-module.

(94) Fix $T \in \mathrm{Hom}_k(V, V)$. For $f(x) \in k[x]$, show that $f(T) \in \mathrm{Hom}_k(V, V)$. In this way, V becomes a $k[x]$-module where $f \cdot v = f(T)v$.
  (a) If $T = 0$, show that $f \cdot v = a_0 v$ where a_0 is the constant coefficient of f.
  (b) Describe the action of $k[x]$ on V when $T = \mathrm{Id}_V$.
(95) Suppose now that M is a $k[x]$-module.
  (a) Show that M is a k-vector space.
  (b) Show that the map from M to M given by $m \mapsto x \cdot m$ belongs to $\mathrm{Hom}_k(M, M)$.
  (c) Suppose that $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in k[x]$. Let M denote the $k[x]$-module $k[x]/(f)$ and denote by $S \in \mathrm{Hom}_k(M, M)$ the linear map that corresponds to $m \mapsto x \cdot m$.
    (i) What is the dimension of M?
    (ii) With respect to the basis $\mathbf{v} = (1, x, x^2, \ldots, x^{\dim(M)-1})$ of M, what is ${}_{\mathbf{v}}[S]_{\mathbf{v}}$?[1]

[1] Suppose $S(x^j) = \sum_{j=0}^{\dim(M)-1} a_{ij} x^i$. The matrix ${}_{\mathbf{v}}[S]_{\mathbf{v}}$ is a $\dim(M) \times \dim(M)$ matrix whose ij^{th} entry is a_{ij}.

(96) Conclude that there is a bijection between the set of $k[x]$-modules and the set of pairs (V, T) where V is a k-vector space and $T \in \mathrm{Hom}_k(V, V)$. [Don't be misled: This has nothing to do with Prompt 95c.]

(97) Suppose that M is a $k[x]$-module. Suppose the action of x on M corresponds to $S \in \mathrm{Hom}_k(M, M)$. Show that the $k[x]$-submodules of M are precisely the S-stable subspaces[1] of M.

The matrix ${}_{\mathbf{v}}[S]_{\mathbf{v}}$ is called the *companion matrix of* $f(x)$. It is often denoted $\mathscr{C}_{f(x)}$.

As the example of $k[x]$-modules makes abundantly clear, a given abelian group can carry many, many different R-module structures. Don't forget this.

Recall that an R-module homomorphism between R-modules M and N is a function from M to N that respects both (a) the group structure of M and N and (b) scalar multiplication. That is:

Definition. Suppose R is a ring and M and N are R-modules. A function $g\colon M \to N$ is called a *R-module homomorphism* provided that

- g is a group homomorphism and
- $g(rm) = rg(m)$ for all $r \in R$ and $m \in M$.

The set of R-module homomorphisms from M to N is denoted $\mathrm{Hom}_R(M, N)$ or $\mathrm{Hom}_{R-mod}(M, N)$.

(98) Are the $\mathbb{Z}$-modules $5\mathbb{Z}$ and $7\mathbb{Z}$ isomorphic as $\mathbb{Z}$-modules?

(99) Suppose I is an ideal in a ring R. Show that the quotient map $R \to R/I$ is an R-module homomorphism.

(100) Suppose R is a commutative ring and M and N are R-modules. Show that $\mathrm{Hom}_R(M, N)$ is an R-module. What if R is not commutative?

(101) Suppose R is a ring, M and N are R-modules, and $f \in \mathrm{Hom}_R(M, N)$. Show that $\ker(f)$, the kernel of f, is a submodule of M. Show that $\mathrm{im}(f)$, the image of f, is a submodule of N.

(102) Suppose R is a commutative ring and M is an R-module. Show that M is naturally a module for the ring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$. What if R is not commutative?

Some Things to Think About

[A] Suppose k is a field and V and W are finite dimensional k-vector spaces with bases $\mathbf{v}$ and $\mathbf{w}$, respectively. The choice of bases gives us a bijective map between $\mathrm{Hom}_k(V, W)$ and $\mathrm{Mat}_{\dim(W)\times\dim(V)}(k)$. Thus, a linear maps between an n-dimensional k-vector space and an m-dimensional k-vector space can be encoded in a natural way by nm numbers. Suppose U is a third k-vector space with basis $\mathbf{u}$. Can you think of a way to encode all k-bilinear maps from $V \times W$ to U?

[B] Recall the definition of an associative algebra:

Defintion. Suppose R is a commutative ring. A set A is called an *associative R-algebra* provided that

- A is an R-module and
- the multiplication map $A \times A \to A$ is R-bilinear and associative.

Every abelian group is a $\mathbb{Z}$-module, and *vice-versa*. What sorts of objects are associative $\mathbb{Z}$-algebras?

[1] A subspace X of M is called *S-stable* provided that $S(X) \subset X$.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 24 Sep 2018
Modules: direct products & direct sums

Vocabulary: direct product, direct sum

Suppose R is a ring. Let J be an indexing set[1] and let $(M_j \mid j \in J)$ be a list of R-modules. We begin by looking at the direct product and direct sum of $(M_j \mid j \in J)$. (We've been through this before, the only new thing this time is that the indexing set J is not assumed to be finite.)

Definition. Suppose R is a ring, I is an indexing set, and $(M_i \mid i \in I)$ is a list of R-modules indexed by I. The *direct product* of the (M_i), denoted $\prod_{i\in I} M_i$ or $\prod_i M_i$, is an R-module with elements and operations defined as followed. An element of $\prod_i M_i$ is a sequence (m_i) where $m_i \in M_i$. The operations on $\prod_i M_i$ are defined as follows: for $r \in R$ and $m = (m_i), m' = (m'_i) \in \prod_i M_i$ we define

- rm to be that element of $\prod_i M_i$ whose jth component is rm_j for $j \in I$; that is $(rm)_j = rm_j$, and
- $m + m'$ to be that element of $\prod_i M_i$ whose jth component is $m_j + m'_j$ for $j \in I$; that is $(m+m')_j = m_j + m'_j$.

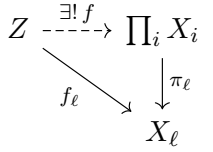
(103) Verify that $\prod_i M_i$ verifies the module axioms.

(104) Show that the set of sequences with entries in $\mathbb{C}$ is a $\mathbb{Q}[\sqrt{2}]$-module. Show that it is isomorphic, as a $\mathbb{Q}[\sqrt{2}]$-module, to $\prod_{n\in\mathbb{N}} \mathbb{C}$.

(105) Let Z be an R-module and let $f_\ell \in \mathrm{Hom}_R(Z, M_\ell)$ for $\ell \in I$. Show that there is a unique $f \in \mathrm{Hom}_R(Z, \prod_i M_i)$ for which $f(z)_j$, the jth component of $f(z)$, is $f_j(z)$ for all $j \in I$.

Prompt 105 sounds like a universal property, and, indeed, in a general category, the universal property of products over an indexing set I looks like:

Universal Property of Direct Products. Suppose $\mathcal{C}$ is a category. Suppose (X_i) is a list of objects in $\mathcal{C}$ indexed by I. A product of the X_i is an object in $\mathcal{C}$, denoted $\prod_i X_i$, together with a list of morphisms $(\pi_j \colon \prod_i X_i \to X_j \mid j \in I)$ satisfying the following universal property: for every object Z in $\mathcal{C}$ and list of morphisms $(f_j \colon Z \to X_j \mid j \in I)$ there exists a unique morphism $f \colon Z \to \prod_i X_i$ such that for all $\ell \in I$ the following diagram commutes:



Products need not exist (consider, again, the category of fields). However, when they do exist, they are, as before, unique up to unique isomorphism.

(106) Suppose Q is an object in $\mathcal{C}$ that, along with a list of morphisms $(\tilde{\pi}_j \colon Q \to X_j \mid j \in I)$, satisfies the universal property of products. Show that there exists a unique isomorphism from Q to $\prod_i X_i$.

We now take up our study of direct sums.

Definition. Suppose R is a ring, I is an indexing set, and $(M_i \mid i \in I)$ is a list of R-modules indexed by I. The *direct sum* of the (M_i), denoted $\oplus_{i\in I} M_i$ or $\bigoplus_i M_i$, is an R-module with elements and operations defined as followed. An element of $\bigoplus_i M_i$ is a sequence (m_i) where $m_i \in M_i$ and $m_i = 0$ for all but finitely many $i \in I$. The operations on $\oplus_i M_i$ are defined as follows: for $r \in R$ and $m = (m_i), m' = (m'_i) \in \oplus_i M_i$ we define

- rm to be that element of $\prod_i M_i$ whose jth component is rm_j for $j \in I$; that is $(rm)_j = rm_j$, and
- $m + m'$ to be that element of $\prod_i M_i$ whose jth component is $m_j + m'_j$ for $j \in I$; that is $(m+m')_j = m_j + m'_j$.

In a direct sum $\bigoplus_i M_i$ one often writes an element $(m_i) \in \bigoplus_i M_i$ as $\sum m_i$ or $\sum' m_i$. Here the prime on the summation sign is added to emphasize that all but finitely many of the m_i are zero. For $j \in I$ we denote by ι_j the natural injection[2] of M_j into $\bigoplus_i M_i$.

(107) Verify that $\bigoplus_i M_i$ satisfies the module axioms.

(108) Verify that $\iota_j \in \mathrm{Hom}_R(M_j, \bigoplus_i M_i)$ for $j \in I$.

(109) Show that if I is finite, then the direct product of $(M_i \mid i \in I)$ and the direct sum of $(M_i \mid i \in I)$ coincide.

[1] **Warning!** J need not be finite. While J could be, for example, $\emptyset$ or $\{1, 2, 43\}$, it could also be, for example, $\mathbb{Z}$, $\mathbb{R}$, or $C^0([0,1])$.

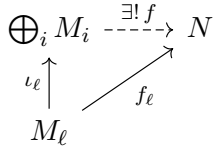
[2] What is it?

(110) Show that the set of sequences with entries in $\mathbb{R}$ is a $\mathbb{R}$-module. Show that it is **not** isomorphic, as an $\mathbb{R}$-module, to $\bigoplus_{n\in\mathbb{N}} \mathbb{R}$. [Hint: What's their dimension? Also, when such questions are asked, it is usually assumed that an isomorphism will respect the natural projections with which both objects are equipped.]

(111) Let N be an R-module and let $f_\ell \in \mathrm{Hom}_R(M_\ell, N)$ for $\ell \in I$. Show that there is a unique $f \in \mathrm{Hom}_R(\oplus_i M_i, N)$ for which $f(\iota_j(m)) = f_j(m)$ for all $j \in I$ and $m \in M_j$.

Prompt 111 sounds like a universal property. In a general category, this becomes the universal property of coproducts[1]; we will stick to the category of modules where the coproduct coincides with the direct sum.

Universal Property of Direct Sums for Modules. Suppose R is a ring, I is an indexing set, and $(M_i \,|\, i \in I)$ is a list of R-modules indexed by I. A direct sum of the M_i is an R-module, denoted $\bigoplus_i M_i$, together with a list of morphisms $(\iota_j \colon M_j \to \bigoplus_i M_i)$ satsifying the following universal property: for every R-module N and list of morphisms $(f_k \colon M_k \to N \,|\, k \in I)$ there exists a unique morphism $f \colon \bigoplus_i M_i \to N$ such that for all $\ell \in I$ the following diagram commutes:



(112) Suppose Q is an R-module that, along with a list of morphisms $(\tilde{\iota}_j \colon M_j \to Q \,|\, j \in I)$, satisfies the universal property of direct sums for R-modules. Show that there exists a unique isomorphism from Q to $\oplus_i M_i$.

(113) Suppose R is a commutative ring. Show that $\mathrm{Hom}_R(\oplus_{i\in I} M_i, N) \simeq \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ as R-modules. What if R is not commutative? *Bonus.* Why not look at $\mathrm{Hom}_R(\prod_{i\in I} M_i, N)$?

(114) *Bonus.* Suppose R is a commutative ring. Show that $\mathrm{Hom}_R(N, \prod_{i\in I} M_i) \simeq \prod_{i\in I} \mathrm{Hom}_R(N, M_i)$ as R-modules.

(115) Suppose S is a set and R is a ring. Let $\mathrm{Fun}'(S, R)$ be the R-module that consists of functions $f \colon S \to R$ for which $f(s) = 0$ for all but finitely many $s \in S$. Show that $\mathrm{Fun}'(S, R) \simeq R^{\oplus S}$ as R-modules.

Something to Think About

Suppose R is a ring. Already for $R = \mathbb{Z}$ we see that not every R-module is isomorphic to $R^{\oplus I} := \bigoplus_{i\in I} R$ for some indexing set I (see also Prompt (122)). In what ways can an R-module fail to look like $R^{\oplus I}$? For which rings might all R-modules look like $R^{\oplus I}$? When is a product $\prod_{i\in I} M_i$ of R-modules isomorphic to $R^{\oplus J}$ for some indexing set J? Is $\prod_{n\in\mathbb{N}} \mathbb{Z}$ isomorphic to a direct sum of copies of $\mathbb{Z}$?

[1] In general, when the arrows are reversed words like "dual" and prefixes like "co" pop up. Can you see why they pop up here?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 26 Sep 2018
Modules: free modules

Vocabulary: submodule generated by a set, generated, finitely generated, cyclic, free, basis, set of free generators, universal property of free modules

Definition. Suppose R is a ring, M is an R-module, and $A \subset M$. The *submodule of M generated by A*, denoted RA, is the R-module whose elements are $\sum_{a\in A} r_a a$ with $r_a \in R$ and $r_a = 0$ for all but finitely many $a \in A$.

By convention, $R\emptyset = \{0\}$. Note that

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m \mid r_1, r_2, \ldots, r_m \in R, a_1, a_2, \ldots, a_m \in A, m \in \mathbb{N}\}.$$

(116) Suppose $A \subset M$. Verify that RA is a submodule of M.
(117) Is it true that $RM = M$?

Definition. Suppose R is a ring and M is an R-module. If N is a submodule of M and $N = RB$ for some $B \subset M$, then we call B a *generating set* for N, and we say that N is *generated* by B. If we can find a finite subset $C \subset M$ for which $N = RC$, the we say that N is *finitely generated*. If N is generated by a singleton set $B = \{b\} \subset M$, then N is said to be *cyclic* and we write $N = Rb$.

(118) Describe $\mathbb{Z}A$ where $A = \{18, 48\}$ is a subset of the $\mathbb{Z}$-module $\mathbb{C}$.
(119) Suppose R is a ring. Is R a finitely generated R-module? Is R/I a finitely generated R-module for $I \subset R$ and ideal? *Bonus.* Is every ideal in R finitely generated?
(120) Suppose R is a commutative nonzero ring. Show that $R[x]$ is not finitely generated as an R-module.
(121) Suppose R is a commutative ring and $f \in R[x]$ is monic of positive degree. Show that $R[x]/(f)$ is finitely generated as an R-module. Do we need to assume f is monic?
(122) Suppose R is a ring and M is a finitely generated R-module. Show that there is a unique largest $d \in \mathbb{Z}_{\geq 0}$ so that if $A \subset R$ and $M = RA$, then $|A| \geq d$. Does it follow that $M = R^{\oplus d} := \bigoplus_{i=1}^{d} R$?

Definition. Suppose R is a ring and M is an R-module. We say that M is *free* provided that there exists $B \subset M$ with the property that for every nonzero $m \in M$ there exists unique nonzero $r_1, r_2, \ldots, r_m \in R$ and unique $b_1, b_2, \ldots, b_m \in B$ for which $m = r_1b_1 + r_2b_2 + \cdots + r_mb_m$. We say that B is a *basis*, *free basis*, or *set of free generators* for M.[a]

[a] **Warning!** In the context of modules, some authors refer to any spanning set as a basis.

Equivalently, M is free provided that there exists $B \subset R$ with the property that for every $m \in M$ there exists unique $(r_b) \in R^{\oplus B} = \bigoplus_{b\in B} R$ for which $m = \sum_{b\in B} r_b b$.

(123) Suppose R is a ring and M is an R-module. Show that M is free if and only if there exists an indexing set I so that $M \simeq R^{\oplus I}$ as R-modules.
(124) Is $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ a free $\mathbb{Z}$-module?
(125) Is the ideal $(2, x)$ in $\mathbb{Z}[x]$ a free $\mathbb{Z}[x]$-module? [Hint: Can two elements of an ideal in a commutative ring be linearly independent?]
(126) Give two examples of $\mathbb{Z}$-modules which are not free. Give two examples of $\mathbb{Z}$-modules which are free.
(127) Suppose M is a $\mathbb{Z}$-module which is not free; can there be an injective $\mathbb{Z}$-module homomorphism from $\mathbb{Z}$ to M?
(128) Suppose k is a field. Is every k-module free? Prove it. *Bonus.* Suppose R is a commutative ring and every R-module is free; must R be a field?
(129) Suppose R is a domain and $I \subset R$ is an ideal.
  (a) If I is not a principal ideal, then can I be a free R-module?
  (b) If I is a principal ideal in R, then must I be a free R-module?
  (c) Suppose A is a PID. Is every submodule of A a free A-module?

Early on in your homework you reviewed the notion of free abelian groups and discussed their universal property. Since modules are 'abelian groups with additional structure' it is not surprising that free R-modules share a similar universal property, namely:

Universal Property of Free Modules. Suppose S is a set. A *free R-module* with basis S is an R-module, denoted $F_R(S)$, together with an injection $\iota\colon S \to F(S)$ such that for every R-module M and every (set) function $f\colon S \to M$ there exists a unique $\tilde{f} \in \mathrm{Hom}_R(F(S), M)$ for which the following diagram commutes.

$$\begin{array}{ccc} S & \xrightarrow{\iota} & F_R(S) \\ & \searrow^{f} & \downarrow{\scriptstyle \exists!\, \tilde{f}} \\ & & M \end{array}$$

(130) (Existence of Free Modules) Suppose S is a set and R is a ring. Recall from Prompt (115) that $\mathrm{Fun}'(S, R)$ denotes the R-module consisting of functions $f\colon S \to R$ for which $f(s) = 0$ for all but finitely many $s \in S$.
  (a) Is $\mathrm{Fun}'(S, R)$ a free R-module?
  (b) Define $\iota'\colon S \to \mathrm{Fun}'(S, R)$ by letting $\iota'(s) = [s]$, the characteristic function of the set $\{s\}$. Show that $\mathrm{Fun}'(S, R)$, together with ι', satisfies the universal property of free modules.

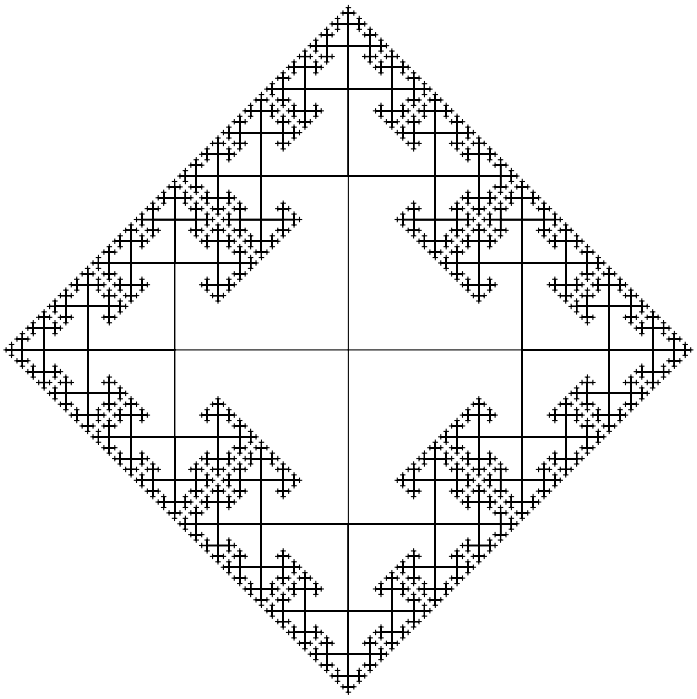
(131) (Uniqueness) Suppose that R is a ring and S is a set. Show that a free R-module with basis S is unique up to unique isomorphism.

Something to Think About

Because modules are 'abelian groups with additional structure', the construction of free objects on a set S is very similar in both the category of abelian groups and the category of R-modules. Suppose that we wanted to look instead at the category of groups and construct a free object on a set S there. The universal property would not be all that different – given S, we'd want a group $F(S)$ together with an injection $\iota\colon S \to F(S)$ such that for every group G and every (set) function $f\colon S \to G$ there exists a unique $\tilde{f} \in \mathrm{Hom}(F(S), G)$ for which the following diagram commutes.

$$\begin{array}{ccc} S & \xrightarrow{\iota} & F(S) \\ & \searrow^{f} & \downarrow{\scriptstyle \exists!\, \tilde{f}} \\ & & G \end{array}$$

If S has one element, this seems to be pretty straightforward – $F(S)$ would be isomorphic to $\mathbb{Z}$. (Why?) However, if S has two elements, say a and b, then $F(S)$ would need to account for all possible products of a, b, a^{-1}, and b^{-1}. (Why?) How to visualize $F(\{a, b\})$? How would you construct a candidate for $F(\{a, b\})$? How would you construct a candidate for $F(S)$ for larger sets S?



Please report any errors you find to smdbackr@umich.edu

Worksheet for 28 Sep 2018
Modules: more on free modules; finitely generated and presented

Vocabulary: linear combination, linearly independent, standard basis, module of relations, finitely presented, presentation, cokernel

We recast the notion of a free R-module in terms that are closer to those used in linear algebra. Remember: for an arbitrary ring, most modules are **not** free.

Definition. Suppose R is a ring, M is an R-module, and $S = (s_i \mid i \in I) \subset M$. A *linear combination* of elements of S (with coefficients in R) is a sum $\sum_{i\in I} r_i s_i$ where $(r_i \mid i \in I)$ is a list of elements in R all but finitely many of which are zero. The elements r_i are called the *coefficients* of the linear combination.

We will sometimes be lazy and write "abfmz" for "all but finitely many of which are zero."

(132) Suppose J is a set. Show that every element of the R-module $\mathrm{Fun}'(J, R)$ is a linear combination of elements of $\{[j] \mid j \in J\}$. (Recall that $[j]$ denotes the characteristic function of the singleton $\{j\}$.)

Definition. Suppose R is a ring and M is an R-module. A list $S = (s_i \mid i \in I) \subset M$ is said to be *linearly independent* (over R) provided that whenever we have a linear combination $\sum_{i\in I} r_i s_i$ which is equal to zero, then $r_i = 0$ for all $i \in I$.

(133) Suppose $R = \mathbb{Z}/6\mathbb{Z}$ and $M = R^{\oplus 2}$. Which of the following lists of elements in M are linearly independent? $((0,0))$, $((1,1))$, $((2,4))$, $((2,4),(3,3))$, $((1,2),(3,1))$, $((1,2),(4,2))$, $((1,1),(1,1))$.

(134) Suppose J is a set. Is $\{[j] \mid j \in J\} \subset \mathrm{Fun}'(J, R)$ linearly independent?

(135) Suppose R is a ring, M is an R-module, and $S = (s_i \mid i \in I) \subset M$ is linearly independent. Show that two linear combinations, $\sum_{i\in I} r_i s_i$ and $\sum_{i\in I} r'_i s_i$, of elements of S are equal if and only if $r_i = r'_i$ for all $i \in I$.

We recall the definition of a free module and basis.

Definition. Suppose R is a ring and M is an R-module. We say that M is *free* provided that there exists $B \subset M$ with the property that for every nonzero $m \in M$ there exists unique nonzero $r_1, r_2, \ldots, r_m \in R$ and unique $b_1, b_2, \ldots, b_m \in B$ for which $m = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m$. We say that B is a *basis* or *set of free generators* for M.

(136) Suppose R is a ring, M is an R-module, and $S = (s_i \mid i \in I) \subset M$. Show that the following are equivalent.
- (a) M is a free module with basis S.
- (b) S generates M (that is, $M = RS$) and S is linearly independent.
- (c) $M \simeq R^{\oplus S}$.
- (d) $M \simeq \mathrm{Fun}'(S, R)$.

(137) Suppose R is a nonzero ring. Show that $M = \{0\}$ if and only if **the** basis for M is $\emptyset$. What goes wrong with this statement if R is the zero ring?

(138) Is $(2, x)$ a linearly independent list in the ideal $I = (2, x)$ in $\mathbb{Z}[x]$?

(139) Let R be a ring and M a free module over R. Let I be a set, and let $(m_i \mid i \in I)$ be a basis of M. Let N be an R-module, and let $(n_i \mid i \in I)$ be a family of elements of N. Show that there is a unique $f \in \mathrm{Hom}_R(M, N)$ such that $f(m_i) = n_i$ for all $i \in I$. If $(n_i \mid i \in I)$ generates N, is f surjective?

Before continuing, we introduce convenient notation.

Suppose R is a ring. The *standard basis* of $R^n = R^{\oplus n}$ is denoted $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ where $e_1 = [1, 0, 0, \ldots, 0, 0]^T$, $e_2 = [0, 1, 0, \ldots, 0, 0]^T$, $\ldots$, $e_n = [0, 0, 0, \ldots, 0, 1]^T$.

(140) Suppose R is a ring and M is a finitely generated R-module, with generators $(m_1, m_2, m_3, \ldots, m_k)$. Define $f \in \mathrm{Hom}_R(R^k, M)$ by setting $f(e_i) = m_i$. Show that f is surjective and the kernel, K, of f is a submodule of $R^{\oplus k}$.

Definition. Suppose R is a ring and M is a finitely generated R-module, with generators $(m_1, m_2, m_3, \ldots, m_\ell)$. Let $f \in \mathrm{Hom}_R(R^\ell, M)$ be the surjective map defined by requiring $f(e_i) = m_i$. The kernel, K, of f is called the *module of relations on* $(m_1, m_2, m_3, \ldots, m_\ell)$.

(141) Why is the kernel of f called the module of relations on $(m_1, m_2, \ldots, m_\ell)$?

Definition. Suppose R is a ring and M is a finitely generated R-module. We say that M is *finitely presented* provided that we can find generators $(m_1, m_2, \ldots, m_\ell)$ for M such that the associated module of relations is finitely generated.

(142) Let $R = \mathbb{Z}[x_1, x_2, x_3, \ldots]$. Let $I = (x_1, x_2, x_3, \ldots)$. Show that R/I is a finitely generated but not finitely presented R-module.

The following ideas are very important and take some getting used to, so start getting used to them. If M is a finitely presented R-module, then we can find generators $(k_1, k_2, \ldots, k_t)$ for $K = \ker(f)$. Let $\mathbf{e}' = (e'_1, e'_2, \ldots, e'_t)$ (resp., $\mathbf{e} = (e_1, e_2, \ldots, e_\ell)$) denote the standard basis for R^t (resp. R^ℓ). In the notation of the definition above, we can create a surjective map $g\colon R^t \twoheadrightarrow K$ by requiring $g(e'_j) = k_j$ for $1 \leq j \leq t$. The composition $\varphi\colon R^t \xrightarrow{g} K \hookrightarrow R^\ell$ is a map between free R-modules and has M as *cokernel*.[1] Every such map between free modules is given by a $\ell \times t$ matrix (whose columns are the images of the standard unit columns under φ) in exactly the same way as in the vector space case – that is, by left multiplication of the $t \times 1$ column matrix to get the $\ell \times 1$ column matrix. We say that this matrix ${}_{\mathbf{e}}[\varphi]_{\mathbf{e}'}$ *presents* M or that the map φ is a *presentation* of M. A goal is to classify modules by understanding these presentations.

(143) Let $R = \mathbb{Z}[x]$. Let $M = R/I$ where $I = (9, 3x, x^2)$.
- (a) Show that M is finitely generated. [Hint: See Prompt 119.]
- (b) Show that M is finitely presented.
- (c) Provide a presentation of M. Choose bases and write down the associated matrix.

Some Things to Think About

[A] Suppose R is a nonzero commutative ring. Suppose $m, n \in \mathbb{N}$ and $\varphi \in \mathrm{Hom}_R(R^m, R^n)$ is injective. Must we have $m \leq n$? What if we remove the assumption that R is commutative?

[B] Suppose M is a finitely presented R-module. By definition there exist finitely generated free R-modules E and F such that

$$E \to F \to M \to 0$$

is exact. Suppose we have another exact sequence

$$0 \to K \to L \to M \to 0$$

with L a finitely generated free R-module. It would be nice if we could conclude that K must be finitely generated; can we? [See Prompt 319.]

[1] In this context, the cokernel is, up to isomorphism, $R^\ell / \mathrm{im}(\varphi)$.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 1 Oct 2018
Modules: presentations

Vocabulary: relations, relation vector, complete set of relations, presented, presentation matrix, Noetherian module, Structure Theorem for Finitely Generated Modules over a PID, invariant factors, free rank

Definition. Suppose R is a ring, M is an R-module, and $(m_1, m_2, \ldots, m_n)$ are elements M. Equations of the form $a_1m_1 + a_2m_2 + \cdots + a_nm_n = 0$ are called *relations* among $m_1, m_2, \ldots, m_n$. The R-vector $[a_1, a_2, \ldots, a_n]^T \in R^n$ is called a *relation* vector.

(144) Consider the $\mathbb{Z}$-module $A = \mathbb{Z}/15\mathbb{Z}$.
  (a) Write down some relation vectors in $\mathbb{Z}$ for the list (1) of elements of A.
  (b) Write down some relation vectors in $\mathbb{Z}^3$ for the list $(10, 6, 1)$ of elements of A.
  (c) Write down some interesting relation vectors in $\mathbb{Z}^2$ for the list $(6, 3)$ of elements of A.

Definition. Suppose R is a ring, M is an R-module, and $(m_1, m_2, \ldots, m_\ell)$ is a list of generators for M. A *complete set of relations* is a set of relation vectors such that every relation vector (with respect to $(m_1, m_2, \ldots, m_\ell)$) occurs as an R-linear combination of elements of the set.

The idea of a 'complete set of relations' can be confusing. I think this is because we are used to thinking of linear algebra from the perspective of images and kernels, and not from the perspective of cokernels.

(145) Suppose R is a ring, M is an R-module, and $(m_1, m_2, \ldots, m_\ell)$ is a list of generators for M. Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_t$ be a set of relation vectors (with respect to $(m_1, m_2, \ldots, m_\ell)$). Suppose $\vec{v}_j = [a_{1j}, a_{2j}, \ldots, a_{\ell j}]^T$. Let A be the $\ell \times t$ matrix whose jth column is $\vec{v}_j$.
  (a) Define $\varphi\colon R^t \to R^\ell$ by $\varphi(\vec{x}) = A\vec{x}$. Show that $\varphi \in \mathrm{Hom}_R(R^t, R^\ell)$.
  (b) Show that if $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_t$ is a complete set of relations (with respect to $(m_1, m_2, \ldots, m_\ell)$), then $M \simeq R^\ell/\varphi(R^t) = R^\ell/AR^t$. [Hint: Define $f \in \mathrm{Hom}_R(R^\ell, M)$ by $f(e_i) = m_i$. Show $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_t$ is a complete set of relations if and only if $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_t)$ generates $\ker(f)$.] *Bonus.* Is the converse true? [See Prompt 320.]

(146) Do your answers in Prompt (144) ever form a complete set of relations? If not, can you fill out your answer to obtain a complete set of relations?

Suppose M is finitely generated. Note that M has a **finite** complete set of relations if and only if M is finitely presented.

Definition. In the notation of Prompt (145): If $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_t$ is a complete set of relations with respect to the list of generators $(m_1, m_2, \ldots, m_\ell)$ for M, then we say that M is *presented* by A and that A is a *presentation matrix* for M.

(147) Find a presentation matrix for the ideal $(2, 1 + \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$. (For uniform notation in discussions, set $R = \mathbb{Z}[\sqrt{-5}]$ and $M = (2, 1 + \sqrt{-5})$.) [Hint: See Homework (80).]

We continue with the notation of Prompt (145). Note that if R were commutative (why?) and we could diagonalize A via invertible matrices $Q \in \mathrm{Mat}_{\ell\times\ell}(R)$ and $P \in \mathrm{Mat}_{t\times t}(R)$, then

$$M \simeq R^\ell/(QAP(R^t)) \simeq \bigoplus_{i=1}^{\ell} R/(a_i)$$

where a_i is the ith diagonal entry of QAP. We are going to spend the next two weeks investigating both when/how we can do this and the consequences of such a diagonalization in some important cases. However, before we take up that study, we establish some fairly general conditions under which a finitely generated module will be finitely presented.

Definition. Suppose R is a ring. An R-module M is called *Noetherian* provided that it satisfies the ascending chain condition. That is, M has no infinite increasing chains of submodules.

Just as for rings (see Homework (59)), there are many equivalent ways to think about Noetherian modules (see Homework (114)). In particular, M is a Noetherian R-module if and only if every submodule of M is finitely-generated.

(148) Suppose R is a ring. Show that a Noetherian R-module need not be finitely presented. [Hint: See Prompt 142.]

When might a finitely generated module be finitely presented? The next several Prompts establish a very useful criterion.

(149) Suppose M is a Noetherian R-module and $L \subset M$ is a submodule. Show that both L and M/L are Noetherian.

(150) Suppose R is a ring, and

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of R-modules. Show that M is Noetherian if and only if both M' and M'' are Noetherian. [Hint: one direction is Prompt 149. For the other direction, note that if L is a submodule of M, then $L/(M' \cap L) \simeq (L + M')/M'$ (why?), and the latter is isomorphic to the image of L in M''.]

(151) Suppose M and N are Noetherian R-modules. Show that $M \oplus N$ is Noetherian. [Hint: Apply Prompt 150 to $0 \to M \to M \oplus N \to N \to 0$.]

(152) Suppose R is Noetherian. Show that R^ℓ is Noetherian.

(153) Suppose R is Noetherian and M is a finitely generated R-module. Show that M is Noetherian.

(154) Conclude that every finitely generated module over a Noetherian ring is finitely presented.

Since every PID is Noetherian (why?), we know that every finitely generated module over a PID is finitely presented. In a week or so, we will prove that, in fact, every such module is isomorphic to a direct sum of finitely many cyclic modules:

Structure Theorem for Finitely Generated Modules over a PID. Suppose R is a PID and M is a finitely generated R module. Then

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus R/(a_3) \oplus \cdots \oplus R/(a_m)$$

for a unique integer $r \geq 0$ and unique proper, nonzero ideals (a_1), (a_2), …, (a_m) of R with $a_1 \mid a_2 \mid \cdots \mid a_m$. We call $a_1, a_2, \ldots, a_m$ (which are unique up to units) the *invariant factors* of M and r is called the *free rank of* M.

The uniqueness of both the free rank and the invariant factors (up to units) immediately implies that if M' is another R-module with the same rank and the same (up to units) invariant factors, then $M \simeq M'$.

(155) What does this result say for linear operators on finite dimensional vector spaces over a field k?

(156) What does this result say about finite abelian groups?

(157) Up to isomorphism, how many abelian groups of order 120 are there?

Something to Think About

In Prompt (157) you described the abelian groups of order 120, up to isomorphism. Suppose that instead of writing down the groups you found in terms of invariant factors, you wanted to do it in terms of elementary divisors (that is, the direction Homework 105 seems to be heading). For example, an abelian group with 45 elements is isomorphic to either $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}15\mathbb{Z}$ or $\mathbb{Z}/45\mathbb{Z}$ in invariant factor form. However, we may want to write the first as $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and the second as $\mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ in elementary divisor form. What might the general result look like for finitely generated modules over a PID? How would we prove it?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 3 Oct 2018
Modules: torsion

Vocabulary: elementary divisors, Spec, exponent, torsion element, regular, $\mathrm{Tor}_R(M)$, torsion free, torsion module, annihilator, $\mathrm{Ann}_R(M)$

We continue our investigation of the Structure Theorem for Finitely Generated Modules over a PID.

Structure Theorem for Finitely Generated Modules over a PID (invariant factor form). Suppose R is a PID and M is a finitely generated R module. Then

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus R/(a_3) \oplus \cdots \oplus R/(a_m)$$

for a unique integer $r \geq 0$ and unique proper, nonzero ideals (a_1), (a_2), …, (a_m) of R with $a_1 \mid a_2 \mid \cdots \mid a_m$. We call $a_1, a_2, \ldots, a_m$ (which are unique up to units) the *invariant factors* of M and r is called the *free rank of* M.

As we hinted at the end of the last worksheet, there is an elementary divisor form of the structure theorem. It follows almost immediately by applying the Chinese Remainder Theorem to the invariant form of the structure theorem (see Homework 116):

Structure Theorem for Finitely Generated Modules over a PID (elementary divisor form). Suppose R is a PID and M is a finitely generated R module. Then

$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus R/(p_3^{\alpha_3}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$$

for a unique integer $r \geq 0$ and the $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ are positive powers of not necessarily distinct primes in R. We call $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ the *elementary divisors* of M; they are unique up to reordering.

I always find the above formulation of the elementary divisor form of the structure theorem to be a bit confusing. I prefer:

$$M \simeq R^r \oplus \left(\bigoplus_{(p) \in \mathrm{Spec}(R) \setminus \{(0)\}} \bigoplus_{n \in I_{(p)}} R/(p^n) \right)$$

where $\mathrm{Spec}(R)$ denotes the set of prime ideals in R and $I_{(p)} = (n_1, n_2, \cdots, n_{k_p})$ is a list of integers with $0 \leq n_1 \leq n_2 \leq \ldots \leq n_{k_p}$. Note that $I_{(p)}$ is the list (0) for all but finitely many $(p) \in \mathrm{Spec}(R)$.

(158) How many abelian groups of order 720 are there? Write them all down in both their invariant factor and elementary divisor form.

(159) How many abelian groups have both of the following properties:
  (a) any minimal generating set has 2 elements
  (b) the exponent[1] is 18.

In homework we have discussed torsion elements in the context of abelian groups. Here is a natural generalization.

Definition. Suppose R is a ring and M is an R-module. An element $m \in M$ is called a *torsion element* of M provided that there exists a non-zero divisor (aka *regular*) $r \in R$ for which $rm = 0$. The set of torsion elements in M is denoted $\mathrm{Tor}_R(M)$; if there is no possibility for confusion, $\mathrm{Tor}_R(M)$ may be denoted $\mathrm{Tor}(M)$ or M_{tor}.

For example, if R is an integral domain, $a \in R \setminus \{0\}$, and $\bar{x} \in R/(a)$, then $a\bar{x} = 0$ and so $\bar{x}$ is a torsion element of $R/(a)$.

Warning: This is not equivalent to the definition given in [DF04, Exercise 4, p. 356]).

Caution: People sometimes refer to the finite order elements of a group, abelian or not, as torsion elements.

(160) Why is the above definition of torsion elements a generalization of that given for abelian groups in the homework?

(161) If $R = M = \mathbb{Z}/6\mathbb{Z}$, then what are the torsion elements of M?

(162) If M is a free R-module, then $\mathrm{Tor}(M) = \{0\}$.

(163) Show: If R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M.

(164) (*Bonus*.) Let A be the free $\mathbb{C}$-module on two (non-commuting) generators ☺ and ☹; note that A is a domain. Define the A-module $M = A/\☺A \oplus A/\☹A$. Consider the elements $m = (1 + \☺A, 0)$ and $m' = (0, 1 + \☹A)$. Show that m and m' are torsion elements, but $m + m'$ is not. Conclude that $\mathrm{Tor}(M)$ is not an A-submodule of M.

[1] The *exponent* of a group is defined to be the least common multiple of the orders of all elements of the group.

Definition. Suppose R is an integral domain and M is an R-module. If $\mathrm{Tor}_R(M) = \{0\}$, then M is said to be *torsion free*. If $\mathrm{Tor}_R(M) = M$, then M is said to be a *torsion module*.

(165) Show that the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a torsion module. Similarly, show that the $k[x]$-module, $k(x)/k[x]$ is a torsion module.

(166) If R is an integral domain, then M/M_{tor} is torsion free.

(167) *Bonus*. More generally: Suppose R is an integral domain with field of fractions K. Show that the R-module K/R is a torsion module.

(168) Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. Is it torsion free? Is it a free $\mathbb{Z}$-module?

(169) Can you reconcile your answer to Prompt 168 with the Structure Theorem for Finitely Generated Modules over a PID?

(170) Is the ideal $(2, x)$ in $\mathbb{Z}[x]$ a torsion free $\mathbb{Z}[x]$-module? Is it a free $\mathbb{Z}[x]$-module?

(171) Can you reconcile your answer to Prompt 170 with the Structure Theorem for Finitely Generated Modules over a PID?

Definition. Suppose R is a ring and M is an R-module. The *annihilator of the R-module M* is

$$\mathrm{Ann}_R(M) := \{r \in R \,|\, rm = 0 \text{ for all } m \in M\}.$$

If no confusion is possible, we will write $\mathrm{Ann}(M)$ rather than $\mathrm{Ann}_R(M)$.

For example, in the elementary divisor form of the structure theorem, we can say that M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of nonzero primes in R.

(172) Suppose R is a commutative ring and M is an R-module. Show that $\mathrm{Ann}(M)$ is an ideal in R.

(173) What is $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z})$?

(174) If A is a finite abelian group, what is $\mathrm{Ann}_{\mathbb{Z}}(A)$?

(175) Can you reconcile your answers to Prompts 173 and 174 with the Structure Theorem for Finitely Generated Modules over a PID?

(176) Suppose R is a ring and

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus R/(a_3) \oplus \cdots \oplus R/(a_m)$$

with $a_1, a_2, \ldots, a_m \in R$.

(a) What is $\mathrm{Ann}(M)$?

(b) Suppose R is an integral domain and $r = 0$. What is $\mathrm{Ann}(M)$?

(c) Suppose R is a PID, $r = 0$, and $a_1 \mid a_2 \mid \cdots \mid a_m$, what is $\mathrm{Ann}(M)$?

Something to Think About

Suppose k is a field, V is a k-module, and $T \in \mathrm{Hom}_k(V, V)$. We know that $k[x]$ is a PID and V is a $k[x]$-module where $xv = T(v)$ for all $v \in V$. What does the structure theorem say in this setting? In the context of Prompt 176c, what might a_m be?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 5 Oct 2018
Modules: rational canonical form

Vocabulary: similar, minimal polynomial, invariant factors, rational canonical form,

Suppose k is a field. Recall that the category of $k[x]$-modules is equivalent to the category of "k-vector spaces with fixed endomorphism" (see Homework 126). Suppose V is a finite dimensional k-vector space and $T \in \mathrm{Hom}_k(V,V)$. Let V_T denote the corresponding $k[x]$-module; note that since V is finite dimensional, V_T is a finitely generated torsion $k[x]$-module. The Structure Theorem for Finitely Generated Modules over a PID (invariant factor form) says that

$$V_T \simeq k[x]/(f_1) \oplus k[x]/(f_2) \oplus k[x]/(f_3) \oplus \cdots \oplus k[x]/(f_m)$$

for unique proper, nonzero ideals (f_1), (f_2), …, (f_m) of $k[x]$ with $f_1 \mid f_2 \mid \cdots \mid f_m$. The unique monic polynomials f_1, f_2, …, f_m are called the the *invariant factors* for T.

(177) Can we write $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$ with $V_i \simeq k[x]/(f_i)$ and each V_i being T-stable?

(178) What is $\deg(f_1) + \deg(f_2) + \cdots \deg(f_m)$? (See also Prompt 195c.)

(179) Suppose $f_i(x) = x^{n_i} + a_{i,n_i-1}x^{n_i-1} + \cdots + a_{i,0} \in k[x]$. Show that with respect to the basis $\mathbf{x} = (1, x, x^2, \ldots, x^{n_i-1})$ of $k[x]/(f_i) \simeq V_i$ we have ${}_{\mathbf{x}}[\mathrm{res}_{V_i} T]_{\mathbf{x}} \in \mathrm{Mat}_{n_i \times n_i}(k)$ is given by the companion matrix

$$\mathscr{C}_{f_i(x)} = \begin{bmatrix} 0 & 0 & 0 & \cdots & \cdots & 0 & -a_{i,0} \\ 1 & 0 & 0 & \cdots & \cdots & 0 & -a_{i,1} \\ 0 & 1 & 0 & \cdots & \cdots & 0 & -a_{i,2} \\ 0 & 0 & 1 & \cdots & \cdots & 0 & -a_{i,3} \\ 0 & 0 & 0 & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & 1 & -a_{i,n_i-1} \end{bmatrix}$$

(180) Show that there is a basis $\mathbf{v}$ of V for which ${}_{\mathbf{v}}[T]_{\mathbf{v}}$ is given by the block-diagonal matrix

$$\begin{bmatrix} \mathscr{C}_{f_1} & & & & \\ & \mathscr{C}_{f_2} & & & \\ & & \mathscr{C}_{f_3} & & \\ & & & \ddots & \\ & & & & \mathscr{C}_{f_m} \end{bmatrix}$$

The matrix in Prompt 180 is the *rational canonical form of* T or the *Frobenius Normal Form of* T. Be sure you understand why it is called canonical. Note that rational canonical form has nothing to do with the rational numbers; the word rational in this context means that it all works without leaving the base field k. Before working out some examples, we point out a useful consequence of rational canonical form.

Definition. Suppose k is a field, V is a finite dimensional k-vector space, and $T \in \mathrm{Hom}_k(V,V)$. The *minimal polynomial* for T is the unique monic polynomial, f, for which $\mathrm{Ann}_{k[x]}(V) = (f(x))$.

(181) In the notation of the definition, why does such an f exist? Why is it unique?

(182) In terms of the structure theorem, what is the minimal polynomial?

(183) Write down the invariant factors for each of the matrices below. What is the rational canonical form for each of the matrices[1]?

$$\begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 \\ 0 & e & 0 & 0 & 0 & 0 \\ 0 & 0 & e & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & 0 & 0 & e \end{bmatrix} \quad \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 \\ 0 & \pi & 0 & 0 & 0 & 0 \\ 0 & 0 & e & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & 0 & 0 & e \end{bmatrix} \quad \begin{bmatrix} e & 0 & 0 & 0 & 0 & 0 \\ 0 & e & 0 & 0 & 0 & 0 \\ 0 & 0 & \pi & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & \pi & 0 \\ 0 & 0 & 0 & 0 & 0 & e \end{bmatrix} \quad \begin{bmatrix} \pi & 0 & 0 & 0 & 0 & 0 \\ 0 & e & 0 & 0 & 0 & 0 \\ 0 & 0 & \pi & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & 0 & 0 & \pi \end{bmatrix} \quad \begin{bmatrix} \pi & 0 & 0 & 0 & 0 & 0 \\ 0 & e & 0 & 0 & 0 & 0 \\ 0 & 0 & \pi & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \pi \end{bmatrix}$$

[1] An $m \times n$ matrix A represents a linear transformation $T \in \mathrm{Hom}_k(k^n, k^m)$ via the map $T(\vec{v}) = A\vec{v}$ where $\vec{v}$ is an $n \times 1$ vector.

We next investigate if every matrix is similar to its rational canonical form. Recall, as above, that the category of $k[x]$-modules is equivalent to the category of "k-vector spaces with fixed endomorphism" (see Homework 126). The objects in this latter category are pairs (V, T) where V is a k-vector space and $T \in \mathrm{Hom}_k(V, V)$. A morphism between two objects (V_1, T_1) and (V_2, T_2) in this category is a map $\varphi \in \mathrm{Hom}_k(V_1, V_2)$ satisfying $\varphi \circ T_1 = T_2 \circ \varphi$.

Definition. Suppose k is a field, V is a k-vector space, and $T, S \in \mathrm{Hom}_k(V, V)$. We say that T and S are *similar* provided that there exists $\phi \in \mathrm{Hom}_k(V, V)^\times$ such that $\phi \circ T = S \circ \phi$.

(184) Suppose $S, T \in \mathrm{Hom}_k(V, V)$ are similar. Show that the corresponding $k[x]$-modules are isomorphic. The converse is true as well, see Homework 120.

(185) Does the definition of similar given above agree with the notion of similar[1] for $n \times n$ matrices?

(186) Is every matrix similar to its rational canonical form? That is, are two matrices similar if and only if they have the same invariant factors?

Rational canonical form appears with great regularity on the QR exams. Be sure you can do problems like the following.

(187) How many similarity classes of 4×4 matrices over $\mathbf{F}_3$ with minimal polynomial $x^2 - a$ exist? Write down their rational canonical forms.

Something to Think About

Suppose A is an $n \times n$ matrix. In Homework 113 you show that A and A^T have the same rational canonical form. Hence, the two matrices are similar. In fact, they are symmetrically similar – that is, there is a symmetric[2] $n \times n$ matrix P for which $A = PA^TP^{-1}$. You now have the tools to prove this, so give it a try.

Suppose that you have found a symmetric P for which $A = PA^TP^{-1}$. Note that we then have

$$(PA^T)^T = AP^T = AP = PP^{-1}AP = PA^T,$$

so PA^T is symmetric. Since $A = (PA^T)P^{-1}$, we conclude that every $n \times n$ matrix can be written as the product of two symmetric matrices!

While applying the Structure Theorem for Finitely Generated Modules over a PID to finitely generated abelian groups is often straight-forward, applying it to canonical forms for transformations (and matrices) is often a bit trickier. The following table summarizes how to translate between the two settings.

Finite Groups	**Matrices**
Decompose a finite abelian group as a direct product of cyclic groups (in invariant factor form)	Determine the rational canonical form of a given matrix
Determine whether two given finite abelian groups are isomorphic	Determine whether two given matrices are similar
Determine all abelian groups of a given order	Determine all similarity classes of matrices over a field with a given characteristic polynomial
Determine all finite abelian groups of rank n and a given exponent	Determine all similarity classes of $n \times n$ matrices over a field with a given minimal polynomial

The use of the word "rank" in this context is highly nonstandard (though [DF04] uses it), we really mean that the size of any minimal generating set of our finite abelian group is n.

[1] Two $n \times n$ matrices A and B are called *similar* provided that $B = P^{-1}AP$ for some invertible $n \times n$ matrix P.

[2] An $n \times n$ matrix P is *symmetric* provided that $P^T = P$.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 8 Oct 2018
Modules: Cayley-Hamilton theorem

Vocabulary: eigenvalue, eigenvector, eigenspace, diagonalizable, characteristic polynomial, Cayley-Hamilton Theorem

We begin by recalling some ideas from linear algebra. Suppose k is a field, V is a k-vector space, and $T \in \mathrm{Hom}_k(V,V)$. We say that $\lambda \in k$ is an *eigenvalue for* T provided that there is a nonzero $v \in V$ for which $T(v) = \lambda v$. If $\mu \in k$ is an eigenvalue for T, then any nonzero element of $V_\mu = \ker(\mu \,\mathrm{Id}_V - T)$ is called an *eigenvector for* T. We call V_μ the *μ-eigenspace* of V. We say that T is *diagonalizable* provided that there is a basis for V consisting of eigenvectors for T.

(188) Suppose T is nilpotent, that is $T^n = 0$ for some $n \in \mathbb{N}$. Describe the possible eigenvalues of T.

(189) Suppose $T^2 + 3T = -\mathrm{Id}_V$. Describe the possible eigenvalues of T.

For the remainder of this worksheet, assume V is a finite dimensional k-vector space.

(190) Suppose $A \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$ and $S_A \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$ is given by $S_A(\vec{x}) = A\vec{x}$ for a 2×1 column matrix $\vec{x}$. For each of the matrices below, describe the eigenvalues and eigenspaces for the corresponding S_A.

(a) $A = \begin{bmatrix} \pi & 0 \\ 0 & \pi \end{bmatrix}$ (b) $A = \begin{bmatrix} \pi & 0 \\ 0 & e \end{bmatrix}$ (c) $A = \begin{bmatrix} e & \sqrt{2} \\ 0 & e \end{bmatrix}$ (d) $A = \begin{bmatrix} e & \sqrt{2} \\ 0 & \pi \end{bmatrix}$

(e) $A = \begin{bmatrix} 0 & \pi \\ e & 0 \end{bmatrix}$ (f) $A = \begin{bmatrix} 0 & \pi \\ -e & 0 \end{bmatrix}$ (g) $A = \begin{bmatrix} \sqrt{2} & \pi \\ e & \sqrt{2} \end{bmatrix}$ (h) $A = \begin{bmatrix} \sqrt{2} & \pi \\ -e & \sqrt{2} \end{bmatrix}$

(191) Fix $\rho \in k$. Show that the following statements are equivalent.

- ρ is an eigenvalue for T.
- $(\rho \,\mathrm{Id}_V - T) \in \mathrm{Hom}_k(V,V)$ is not injective.
- $(\rho \,\mathrm{Id}_V - T)$ is not surjective.
- $(\rho \,\mathrm{Id}_V - T)$ is not an isomorphism.
- $\det(\rho \,\mathrm{Id}_V - T) = 0$.
- ρ is a root for $\chi_T(x) = \det(x \,\mathrm{Id}_V - T)$, the *characteristic polynomial of* T.
- $V_\rho \neq \{0\}$.

(192) Compute the characteristic polynomial of S_A for each A that occurs in Prompt 190.

(193) If λ is the only eigenvalue for T, is it true that $V = V_\lambda$?

Recall that V_T denotes the $k[x]$-module associated to the pair (V,T).

(194) Show that $\gamma \in k$ is an eigenvalue for T if and only if $(x-\gamma)\colon V_T \to V_T$ has nontrivial kernel.

We now explore how the minimal polynomial of T and the characteristic polynomial of T are related. Since V is finite dimensional, V_T is a finitely generated torsion $k[x]$-module. The Structure Theorem for Finitely Generated Modules over a PID (invariant factor form) says that

$$V_T \simeq k[x]/(f_1) \oplus k[x]/(f_2) \oplus k[x]/(f_3) \oplus \cdots \oplus k[x]/(f_m)$$

for unique monic polynomials (aka invariant factors) $f_1, f_2, \ldots, f_m$ of $k[x]$ with $f_1 \mid f_2 \mid \cdots \mid f_m$. In Prompt 182 we found that f_m is the minimal polynomial of T; that is f_m is the (unique) minimal degree monic polynomial for which $f(T) = 0$.

(195) Roots and eigenvalues.

(a) Suppose $p \in k[x]$ is the minimal polynomial for T. Suppose $\alpha \in k$ is a root of p. Show that α is an eigenvalue of T. [Hint: Write $p = (x-\alpha)q$. Since p is minimal, q cannot annihilate V ....]

(b) Suppose $p \in k[x]$ is the minimal polynomial for T. If α is an eigenvalue for T, show that $p(\alpha) = 0$.

(c) Show that the characteristic and minimal polynomials of T have the same roots, except for multiplicities.

(196) If $p \in k[x]$ and $S \in \mathrm{Hom}_k(V,V)^\times$, show that $p(STS^{-1}) = Sp(T)S^{-1}$. Conclude that T and STS^{-1} have the same minimal polynomials and the same characteristic polynomials.

(197) Characteristic polynomials and invariant factors.

(a) Suppose $f \in k[x]$ has positive degree. Show that the characteristic polynomial of its companion matrix, $\mathscr{C}_f$, is f.

(b) Use Prompts 196 and 186 to show that $\chi_T(x) = f_1(x)f_2(x)\cdots f_m(x)$.

(c) Write down the rational canonical form of S_A for each A that occurs in Prompt 190.

(198) (*Cayley-Hamilton Theorem*). Use Prompts 195, 196, and 197 to show that $\chi_T(T) = 0$.

Something to Think About

Please report any errors you find to smdbackr@umich.edu

The Cayley-Hamilton Theorem is a very powerful tool (see, for example, Homework 128) and it holds for matrices with entries in any commutative ring R. In the latter context it says is that if R is a commutative ring and $\phi \in \mathrm{Hom}_R(R^n, R^n)$, then $\chi_\phi(\phi) = 0$. There are several very slick proofs of this, can you prove it?

More generally, if M is any finitely generated R-module then one can show that if $\phi \in \mathrm{Hom}_R(M, M)$ and M is generated by n elements, then there exist $a_1, a_2, \cdots, a_n \in R$ such that

$$\phi^n + a_1\phi^{n-1} + a_2\phi^{n-2} + \cdots + a_n = 0.$$

In fact, if I is an ideal in R and $\phi(M) \subset IM$ then we can take $a_j \in I^j$.

This can be further generalized to Nakayama's Lemma, a result of fundamental importance in commutative algebra:

> Suppose A is a commutative ring. Let $\mathfrak{a}$ be an ideal in A, and let N be a finitely-generated module over A. If $\mathfrak{a}N = N$, then there exists an $r \in 1 + \mathfrak{a}$ such that $rN = \{0\}$.

Can you show that Nakayama's Lemma implies the Cayley-Hamilton Theorem?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 10 October
Modules: Jordan form

Vocabulary: elementary divisors, Jordan block, Jordan canonical form, geometric multipliciy, semisimple

Suppose k is a field. Recall that the category of $k[x]$-modules is equivalent to the category of "k-vector spaces with fixed endomorphism" (see Homework 126). *Suppose V is a finite dimensional k-vector space and $T \in \mathrm{Hom}_k(V,V)$.* Let V_T denote the corresponding $k[x]$-module; note that since V is finite dimensional, V_T is a finitely generated torsion $k[x]$-module. The Structure Theorem for Finitely Generated Modules over a PID (elementary divisor form). says that

$$V_T \simeq k[x]/(p_1^{\alpha_1}) \oplus k[x]/(p_2^{\alpha_2}) \oplus k[x]/(p_3^{\alpha_3}) \oplus \cdots \oplus k[x]/(p_s^{\alpha_s})$$

where $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ are positive powers of not necessarily distinct monic irreducibles in $k[x]$. We call $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ the *elementary divisors* of T; they are unique up to reordering.

(199) Can we write $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$ with $V_i \simeq k[x]/(p_i)^{\alpha_i}$ and each V_i being T-stable?

(200) Show $\alpha_1 \cdot \deg(p_1) + \alpha_2 \cdot \deg(p_2) + \cdots + \alpha_s \cdot \deg(p_s) = \dim(V)$ and $\chi_T(x) = \prod_{i=1}^s p_i^{\alpha_i}(x)$.

(201) Suppose $A \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$ and $S_A \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$ is given by $S_A(\vec{x}) = A\vec{x}$ for a 2×1 column matrix $\vec{x}$. For each of the matrices below, describe the elementary divisors of S_A.

(a) $A = \begin{bmatrix} \pi & 0 \\ 0 & \pi \end{bmatrix}$ (b) $A = \begin{bmatrix} \pi & 0 \\ 0 & e \end{bmatrix}$ (c) $A = \begin{bmatrix} e & \sqrt{2} \\ 0 & e \end{bmatrix}$ (d) $A = \begin{bmatrix} e & \sqrt{2} \\ 0 & \pi \end{bmatrix}$

(e) $A = \begin{bmatrix} 0 & \pi \\ e & 0 \end{bmatrix}$ (f) $A = \begin{bmatrix} 0 & \pi \\ -e & 0 \end{bmatrix}$ (g) $A = \begin{bmatrix} \sqrt{2} & \pi \\ e & \sqrt{2} \end{bmatrix}$ (h) $A = \begin{bmatrix} \sqrt{2} & \pi \\ -e & \sqrt{2} \end{bmatrix}$

For the remainder of this worksheet, assume χ_T factors completely into linear factors over k.

Since $\chi_T(x)$ factors into linear factors, each p_i is of the form $(x - \lambda_i)$ for some eigenvalue λ_i of T.

(202) Suppose that $p_i^{\alpha_i}(x) = (x-\lambda_i)^{\alpha_i} \in k[x]$. Show that with respect to the basis $\mathbf{x} = ((x-\lambda)^{\alpha_i - 1}, (x-\lambda)^{\alpha_i - 2}, \ldots, (x-\lambda)^2, (x-\lambda), 1)$ we have ${}_{\mathbf{x}}[\mathrm{res}_{V_i} T]_{\mathbf{x}} \in \mathrm{Mat}_{\alpha_i \times \alpha_i}(k)$ is given by the matrix

$$J_{\lambda_i,\alpha_i} = \begin{bmatrix} \lambda_i & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \lambda_i & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{bmatrix}$$

[Hint: $x = \lambda + (x - \lambda)$. Also, why is $\mathbf{x}$ a basis?]

Definition. The matrix J_{λ_i,α_i} is the *Jordan block* of size α_i corresponding to λ_i.

(203) Show that there is a basis $\mathbf{v}$ of V for which ${}_{\mathbf{v}}[T]_{\mathbf{v}}$ is given by the block-diagonal matrix

$$\begin{bmatrix} J_{\lambda_1,\alpha_1} & & & & \\ & J_{\lambda_2,\alpha_2} & & & \\ & & J_{\lambda_3,\alpha_3} & & \\ & & & \ddots & \\ & & & & J_{\lambda_s,\alpha_s} \end{bmatrix}$$

The matrix in Prompt 203 is the *Jordan canonical form of T*. It is not as canonical as the rational canonical form: over most fields there is no way to choose the order of the different Jordan blocks that occur.

(204) Express $\chi_T(x)$ as a product of the elementary divisors of T; if your answer is not expressed entirely in terms of x and the eigenvalues of T, then try again. In terms of your fomula for $\chi_T(x)$, what does it mean that the monic irreducibles p_i are not necessarily distinct?

(205) Suppose $A, B \in \mathrm{Mat}_{n\times n}(k)$ and both χ_A and χ_B factor completely into linear factors. If the Jordan canonical form or A and B agree (up to ordering of Jordan blocks), then are A and B similar?

(206) Suppose λ is an eigenvalue of T. Show that $\dim_k(V_\lambda)$, the *geometric multiplicity of* λ, is equal to the number of Jordan blocks corresponding to λ in the Jordan canonical form of T.

Nilpotent transformations play an important role in many areas of mathematics.

(207) Does a nilpotent transformation T always have a Jordan form?

(208) Characterize the nilpotent matrices in $\mathrm{Mat}_{n\times n}(k)$ in terms of their Jordan canonical form.

(209) Suppose k is a field and $A \in \mathrm{Mat}_{n\times n}(k)$. Suppose $j \in \mathbb{Z}_{\geq 0}$ has the property that $A^{j+1} = 0$ and $A^j \neq 0$. Show $j \leq n$.

(210) Show that the Jordan canonical form of A can be written as $A_s + A_n$ where (i) A_s is diagonalizable, (ii) A_n is nilpotent, and (iii) $A_sA_n = A_nA_s$. Conclude that T has a similar decomposition $T = T_s + T_n$.

The subscript n stands for nilpotent, what about the s?

Definition. Suppose k is a field, W is a finite dimensional k-vector space, and $S \in \mathrm{Hom}_k(V, V)$.We say that S is *semisimple* provided that its minimal polynomial is a square free product of irreducible monic polynomials in $k[x]$.

Note that the minimal polynomial for A_S (and hence T_s) has distinct roots, hence S is semisimple.

(211) Suppose k is a field, W is a k-vector space, and $\phi \in \mathrm{Hom}_k(W, W)$. If ϕ is both semisimple and nilpotent, then what is ϕ?

(212) (*Bonus*). Suppose W is a finite dimensional k-vector space and $\phi \in \mathrm{Hom}_k(W, W)$. Show that ϕ is semisimple if and only if every ϕ-stable subspace has a ϕ-stable complement. That is, if $X \subset W$ is a ϕ-stable subspace of W, then there exists a ϕ-stable subspace $Y \subset W$ for which $W = X + Y$ and $X \cap Y = \{0\}$.

Something to Think About

Under the assumption that χ_T factors completely into linear factors, in Prompt 210 we wrote $T = T_s + T_n$ where $T_s \circ T_n = T_n \circ T_n$, T_s is semisimple, and T_n is nilpotent. T_s is usually called the semisimple part of T and T_n is called the nilpotent part of T. This decomposition is called a *Jordan-Chevalley decomposition* of T. For perfect fields[1] such a decomposition holds even when χ_T doesn't completely factor into linear factors.

Here are some facts about this decomposition:

- The decomposition is unique.
- There exist $f, g \in k[x]$ such that $T_s = f(T)$ and $T_n = g(T)$. [This immediately implies that any element of $\mathrm{Hom}_k(V, V)$ that commutes with T must also commute with both T_s and T_n.]
- If $U \subset W \subset V$ and $T(W) \subset U$, then $T_s(W) \subset U$ and $T_n(W) \subset U$.

How many of these facts can you prove? (See Homework 129.)

[1] A field F is said to be *perfect* provided that every irreducible polynomial over F has distinct roots. Math 594 will have much more to say about perfect fields. Every finite field and every characteristic zero field is perfect.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 12 & 17 October
Modules: Structure Theorem for Finitely Generated Modules over a PID

Vocabulary: composition series, composition factors, length

The series of Homework problems that includes exercises (70), (82), (103), (117), and (127) provides an algorithmic proof of the Structure Theorem for Finitely Generated Modules over a PID (invariant factor form):

Structure Theorem for Finitely Generated Modules over a PID (invariant factor form). Suppose R is a PID and M is a finitely generated R module. Then

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus R/(a_3) \oplus \cdots \oplus R/(a_m)$$

for a unique integer $r \geq 0$ and unique proper, nonzero ideals (a_1), (a_2), …, (a_m) of R with $a_1 \mid a_2 \mid \cdots \mid a_m$.

An outline of the proof: Suppose the finitely generated module M is presented by some $\ell \times t$ matrix A with entries in R. If this matrix is diagonal, then it follows immediately that its cokernel, which is isomorphic to M, is a direct sum of cyclic modules $R/(a_i)$. So we want to show that over a PID we can choose a generating set for M and a generating set for the module of relations K in such a way that A is diagonal. In Homework (127) you proved that changing the generators for M (respectively K) amounts to multiplying A on the right (respectively left) by an invertible matrix over R. In Homework (70) you saw how to diagonalize (small) A algorithmically over $\mathbb{Z}$ using EROs and ECOs. In Homework (82) you saw how to diagonalize A algorithmically over Euclidean domains using EROs and ECOs. In Homework (103) you saw how to diagonalize A algorithmically over PIDs using EROs and ECOs and an additional invertible transformation. In Homework (117) you proved the uniqueness statement of the structure theorem. This approach to the Structure Theorem for Finitely Generated Modules over a PID (invariant factor form) is useful for performing computations – be sure that you can carry it out in practice. In [DF04, pp. 480–481] the algorithm is discussed for finitely generated torsion $k[x]$-modules.

In Homework 116 you used the Chinese Remainder Theorem to derive the elementary divisor form of the Structure Theorem for Finitely Generated Modules over a PID:

Structure Theorem for Finitely Generated Modules over a PID (elementary divisor form). Suppose R is a PID and M is a finitely generated R module. Then

$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus R/(p_3^{\alpha_3}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$$

for a unique integer $r \geq 0$ and the $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ are positive powers of not necessarily distinct primes in R.

The conclusion of the elementary divisor form of the structure theorem may be recast as

$$M \simeq R^r \oplus \left(\bigoplus_{(p) \in \mathrm{Spec}(R) \setminus \{(0)\}} \; \bigoplus_{n \in I_{(p)}} R/(p^n) \right)$$

where $\mathrm{Spec}(R)$ denotes the set of prime ideals in R and $I_{(p)} = (n_1, n_2, \cdots, n_{k_p})$ is a list of integers with $0 \leq n_1 \leq n_2 \leq \ldots \leq n_{k_p}$. Note that $I_{(p)}$ is the list (0) for all but finitely many $(p) \in \mathrm{Spec}(R)$.

(213) Prove that the elementary divisor form of the structure theorem may be recast as claimed.

The Prompts below outline another proof of the structure theorem.

(214) Suppose R is a PID and M is a torsion free finitely-generated R-module. Show that M is free. [Hint: Let ℓ be the cardinality of a maximal linearly independent subset of M. Use Homework 110 to show M is isomorphic to a submodule of R^ℓ. Homework 121 may be useful.]

(215) Suppose R is a PID and M is a finitely generated R-module. From Prompt 166 we know M/M_{tor} is free; say $M/M_{\text{tor}} \simeq R^r$.
  (a) Show $M \simeq M_{\text{tor}} \oplus R^r$.
  (b) Is r unique? Why?
  [Hint: Homework 107 and Homework 47 may be useful.]

Prompt 215 shows that if M is a finitely generated module over a PID, then M_{tor} is finitely generated. We already knew this. Indeed, since R is a PID, from Prompt 60 it is Noetherian. From Prompt 153 we know that every finitely generated module over a PID is Noetherian. Thus, $M_{\text{tor}} \leq M$ is finitely generated.

(216) (Chinese Remainder Theorem for finitely generated torsion modules over a PID) Suppose R is a PID and M is a fintely generated R-module. Show

$$M_{\text{tor}} \simeq \bigoplus_{(p)\in \text{Spec}(R)\setminus\{(0)\}} M(p).$$

[Hint: Mimic your proof of Homework 118.] Is it necessary to assume that M is finitely generated? What is $M(0)$?

(217) Suppose R is a PID, M is a finitely generated R-module, and $(p) \in \text{Spec}(R) \setminus \{(0)\}$. Let $y_1, y_2, \ldots, y_n$ be a set of generators for $M(p)$. Thanks to Homework 124 we have $\text{Ann}_R(y_j) = (p^{k_j})$ for $k_j \in \mathbb{Z}_{\geq 0}$. WOLOG, $k_1 \leq k_2 \leq \cdots \leq k_n$.

(a) Show $(M(p)/\langle y_n\rangle)(p) = M(p)/\langle y_n\rangle$.

(b) Suppose $\bar{x} \in M(p)/\langle y_n\rangle$ and $\text{Ann}_R(\bar{x}) = (p^e)$.

(i) Show $e \leq k_n$.

(ii) Show there exists $x \in M(p)$ projecting to $\bar{x}$ such that $\text{Ann}_R(\bar{x}) = \text{Ann}_R(x) = (p^e)$.

(218) Suppose R is a PID, M is a finitely generated R-module, and $(p) \in \text{Spec}(R) \setminus \{(0)\}$ with $M(p) \neq \{0\}$. Show that there exists unique $e_1, e_2, \ldots, e_n$ in $\mathbb{Z}_{>0}$ with $e_1 \leq e_2 \leq \cdots \leq e_n$ so that

$$M(p) \simeq R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_n}).$$

Moreover, any generating set for $M(p)$ has n or more elements. [Hint: For uniqueness you may want to use Prompt 58, Homework 98, and Homework 47. For existence, you may want to use induction on the minimal set of generators together with Homework 123 and Prompt 217.]

(219) Conclude that the Structure Theorem for Finitely Generated Modules over a PID (elementary divisor form) is true.

Just as the elementary divisor form of the structure theorem followed without too much trouble from the invariant factor theorem (see Homework 116), going in the reverse direction is also relatively straightforward.

(220) Suppose $M_{\text{tor}} \simeq \oplus M(p_j)$ where $p_1, p_2, \ldots p_m \in \text{Spec}(R)$ are distinct and $M(p_j) \neq \{0\}$. For each p_j, write

$$M(p_j) \simeq R/(p_j^{e_{j,1}}) \oplus R/(p_j^{e_{j,2}}) \oplus \cdots \oplus R/(p_j^{e_{j,n_j}}).$$

with $0 < e_{j,1} \leq e_{j,2} \leq \cdots \leq e_{j,n_j}$.

(a) Show $a_m = \prod_{j=1}^{m} p_j^{e_{j,n_j}}$ is the annhilator of $M(p)$.

(b) How to define the $a_{m-1}, a_{m-2}, \ldots, a_1$ occurring in the invariant factor form of the structure theorem?

(c) *Bonus.* Show that this works.

Some things to Think About

[A] While PIDs are a fairly large class of rings, many interesting rings are not PIDs. For example, most of the rings that arise in representation theory aren't commutative. What sort of structure theorems might exist in these more general settings? The Jordan-Hölder Theorem is one example of such a result. To state it, we need to expand our vocabulary a bit.

Let R be a ring. We call an R-module N *simple* provided that the only submodules of N are $\{0\}$ and N. A *composition series* for an R-module M is a finite chain of submodules

$$\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_k = M$$

for which M_{j+1}/M_j is simple for all j. The R-modules M_{j+1}/M_j are called *the composition factors* of the composition series and k is called the *length* of the composition series.

Suppose M is an R-module that admits a composition series. The Jordan-Hölder Theorem states that (a) any given chain of submodules of M can be refined to a composition series, (b) any two composition series of M have the same length, and (c) any two composition series of M have the same composition factors up to rearrangement and isomorphism.[1]

How is this a generalization? How might you prove this? What conditions on M will guarantee that M admits a composition series? Are there rings for which every finitely generated module admits a composition series?

[B] Does the functorial map from a finitely generated abelian group G to its torsion-free quotient G/G_{tor} have a functorial splitting?

[1] The Hölder program, named for Otto Hölder, asked for a classification of all finite simple groups – do you see how this is connected to the Jordan-Hölder Theorem?

Please report any errors you find to smdbackr@umich.edu

Worksheet[1] for 22 Oct 2018
Tensor products

> [I]t is the things you _can_ prove that tell you how to think about tensor products. In other words, you let elementary lemmas and examples shape your intuition of the mathematical object in question. There's nothing else, no magical intuition will magically appear to help you "understand" it.
>
> –Johan de Jong, in the comments to Cathy O'Neil's post *What tensor products taught me about living my life*[2]

Vocabulary: tensor product, tensors, bilinear, pure tensor, elementary tensor, rank-one tensor

Suppose R is a commutative ring[3] with identity and L, M, N, and P are unital R-modules.

We know how to "add" M and N: we just look at the direct sum $M \oplus N$. Tensor products may be thought of as an answer to the question: how to "multiply" M and N? The tensor product of M and N will be denoted by $M \otimes_R N$. Elements of $M \otimes_R N$ will be called *tensors* and look like $\sum r_i(m_i \otimes n_i)$ with $r_i \in R$ (abfmz), $m_i \in M$ and $n_i \in N$. We call $m_i \otimes n_i$ a *pure tensor* or *elementary tensor* or *rank-one tensor*; since the pure tensors span $M \otimes_R N$, it is often[4] enough to understand how things work for them and "extend by linearity" to the whole of $M \otimes_R N$.

(221) Since we want to "multiply" M and N, we probably should require some version of the distribution laws – what would those look like (in terms of elementary tensors)?

In addition to the analogue of the distribution laws, we also want:

(*) $$r(m \otimes n) = (rm) \otimes n = m \otimes (rn) \quad \text{for } r \in R,\ m \in M, \text{ and } n \in N.$$

The tensor product of M and N is going to be an R-module that is, in some appropriate sense, as free as possible and satisfies the relations encoded in both Equation (*) and your answer to Prompt (221). You have encountered these types of relations before (think about the dot product, the Hilbert-Schmidt inner product, a general inner product, matrix multiplication, the cross product, ...). The mathematical term for them is *bilinear*:

Definition. A map $B\colon M \times N \to P$ is said to be bilinear provided that B is linear in each variable, that is

- $B(rm, n) = rB(m, n)$ and $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$
- $B(m, rn) = rB(m, n)$ and $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$

for all $r \in R$, $m, m_1, m_2 \in M$, and $n, n_1, n_2 \in N$.

From our discussion thus far, we should require the map from $M \times N$ to $M \otimes_R N$ that sends (m, n) to $m \otimes n$ to be bilinear.

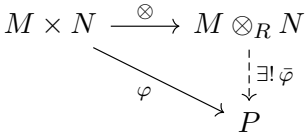
(222) If $B\colon M \times N \to L$ is bilinear and $f \in \mathrm{Hom}_R(L, P)$, then $f \circ B\colon M \times N \to P$ is bilinear.

(223) Suppose $n \in \mathbb{Z}_{>1}$. Show that the map $B\colon R^n \times R^n \to \mathrm{Mat}_n(R)$ defined by $B(v, w) = vw^T$ is bilinear. Show that, in general, the image of B is not a submodule of $\mathrm{Mat}_n(R)$. [Hint: What is the rank of $B(v, w)$?]

(224) Suppose $B\colon M \times N \to P$ is bilinear. Is $\ker(B)$ a submodule?

Motivated by Prompt (222) and our quest for the freest R-module that satisfies both Equation (*) and your answer to Prompt (221) we introduce the following universal property.

Universal Property of tensor products. The *tensor product* $M \otimes_R N$ is an R-module with a bilinear map $\otimes\colon M \times N \to M \otimes_R N$ such that for every bilinear map $\varphi\colon M \times N \to P$ there is a unique linear map $\bar{\varphi} \in \mathrm{Hom}_R(M \otimes_R N, P)$ for which the following diagram commutes.



As a candidate for the tensor product of M and N, look at the R-module $T := F_R(M \times N)/S$ where S is the submodule of $R^{\oplus(M\times N)} = F_R(M \times N)$ generated by $\iota(rm, n) - r\iota(m, n)$, $\iota(m, rn) - r\iota(m, n)$, $\iota(m_1, n) + \iota(m_2, n) - \iota(m_1 + m_2, n)$, and $\iota(m, n_1) + \iota(m, n_2) - \iota(m, n_1 + n_2)$. Here $\iota\colon M \times N \to R^{\oplus(M\times N)}$ is the natural (set) inclusion map.

---

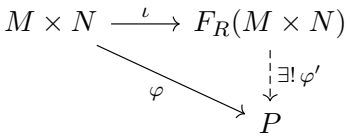
[1] The development here follows Keith Conrad's *Tensor Products*.

[2] mathbabe.org/2011/07/20/what-tensor-products-taught-me-about-living-my-life/

[3] Note that [DF04] does not assume that R is commutative. When R is not commutative, the tensor product is not, in general, an R-module. However, it is always an abelian group. Tensor products over non-commutative rings come up all the time in, for example, representation theory. It is challenging enough to come to grips with tensor products over a commutative ring, so we'll focus our attention on this case.

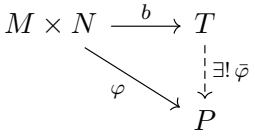
[4] Though not always!

(225) The universal mapping property of free modules allows us to extend φ to a unique linear φ' so that the diagram



commutes. Use the bilinearity of φ to show that $S \subset \ker \varphi'$.

(226) Use the universal property of quotients to conclude that there is a unique linear $\bar{\varphi}$ so that the diagram



commutes. Wait! What is the map b in this diagram? Is it bilinear?

(227) Show that if (T', b') also satisfies the universal property of tensor products, then there is a unique isomorphism from T to T'. Because of this uniqueness, we refer to the pair $(M \otimes_R N, \otimes)$ as *the* tensor product of M and N. [Hint: Id_T is the unique linear map for which $b = \mathrm{Id}_T \circ b \ldots$]

"I wasn't asking much: I just wanted to figure out the most basic properties of tensor products. And it seemed like a moral issue. I felt strongly that if I really really wanted to feel like I understand this ring, which is after all a set, then at least I should be able to tell you, with moral authority, whether an element is zero or not. For f***s sake!"

– Cathy O'Neil in her post *What tensor products taught me about living my life*[1]

(228) Practice with the definitions.

(a) Since $M \otimes_R N$ is an R-module (how?), every element of $M \otimes_R N$ is a linear combination of elementary tensors. Show that if $(m_i \mid i \in I)$ spans M and $(n_j \mid j \in J)$ spans N, then $(m_i \otimes n_j \mid i \in I \text{ and } j \in J)$ spans $M \otimes_R N$.

(b) Show that $R \otimes_R M \simeq M$.

(c) Show that $N \otimes_R M \simeq M \otimes_R N$.

(d) Show that a simple tensor $m \otimes n \in M \otimes_R N$ is zero if and only if for every bilinear map $\varphi\colon M \times N \to P$ we have $\varphi(m, n) = 0$. Conclude that $m \otimes 0 = 0 \otimes n = 0$.

(e) Show that $\sum_i r_i m_i \otimes n_i \in M \otimes_R N$ is zero if and only if for every bilinear map $\varphi\colon M \times N \to P$ we have $\sum_i r_i \varphi(m_i, n_i) = 0$.

(f) Show that $M \otimes_R N = 0$ if and only if for every bilinear map $\varphi\colon M \times N \to P$ we have $\varphi = 0$.

(229) Examples that hurt one's brain a bit.

(a) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/43\mathbb{Z} = 0$.

(b) Show that if A is a finite abelian group, then $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

(c) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

(d) Show that $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) = 0$

(e) Show that $(\mathbb{Z}/43\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/43\mathbb{Z}) \neq 0$. (*Bonus*: What is it?)

Some Things to Think About

[A] Suppose k is a field and V, W are k-vector spaces. If $(v_i \mid i \in I)$ is a basis for V and $(w_j \mid j \in J)$ is a basis for W, then we know from Prompt (228a) that $(v_i \otimes w_j \mid i \in I \text{ and } j \in J)$ spans the k-vector space $V \otimes_k W$. Is it a basis? For what class of rings and modules would you expect a basis for the tensor product to arise in this way?

[B] If you have ever studied tensors in physics (always with $R \in \{\mathbb{R}, \mathbb{C}\}$), what is the relation between the tensor product we've discussed today and the tensors you encountered in physics?

[1] mathbabe.org/2011/07/20/what-tensor-products-taught-me-about-living-my-life/

Please report any errors you find to smdbackr@umich.edu

Worksheet[1] for 24 Oct 2018
Tensor products: practice

The goal today is to gain some intuition about tensor products and drive home this important point: universal properties can help you avoid much grief. Suppose R is a commutative ring.

(230) Suppose E and F are free R-modules. Let $(e_i \mid i \in I)$ and $(f_j \mid j \in J)$ be bases for E and F respectively.
- (a) Suppose $v = \sum_i v_i e_i \in E$ (abfmz) and $w = \sum_j w_j f_j \in F$ (abfmz). For $i_0 \in I$ and $j_0 \in J$ define $B_{i_0 j_0} : E \times F \to R$ by $B(v, w) = v_{i_0} w_{j_0}$. Show that this map is bilinear.
- (b) Use the universal property of tensor products to conclude that there is a unique linear map $\bar{B}_{i_0 j_0} : E \otimes_R F \to R$ for which $\bar{B}_{i_0 j_0}(v \otimes w) = v_{i_0} w_{j_0}$.
- (c) Show that $(e_i \otimes f_j \mid i \in I \text{ and } j \in J)$ is linearly independent.
- (d) Use Prompt (228a) to conclude that $(e_i \otimes f_j \mid i \in I \text{ and } j \in J)$ is a linearly independent spanning set for $E \otimes_R F$. Conclude that $E \otimes_R F$ is a free R-module.
- (e) If k is a field and V, W are finite dimensional k-vector spaces, what is the dimension of $V \otimes_k W$?
- (f) (*Bonus.*) Show that $R[X] \otimes_R R[Y]$ is isomorphic to $R[X, Y]$.

(231) Elementary or not?[2]
- (a) Suppose I is an ideal in R. Show that all tensors in $R/I \otimes_R M$ are elementary.
- (b) Show that not every element of the $\mathbb{R}$-module $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is elementary. [Hint: Use the result of Prompt (230d)]
- (c) Suppose k is a field and $n \in \mathbb{Z}_{>1}$. Recall from Prompt (223) that $B : k^n \times k^n \to \mathrm{Mat}_n(k)$ defined by $B(v, w) = vw^T$ is bilinear but its image is not a submodule of $\mathrm{Mat}_n(k)$. Show that the unique linear map $\bar{B} : k^n \otimes_k k^n \to \mathrm{Mat}_n(k)$ for which $B = \bar{B} \circ \otimes$ is an isomorphism. What does this tell you about the elementary tensors in $k^n \otimes_k k^n$? [Hint: With respect to the standard basis of k^n, what is $e_i e_j^T$?]

(232)
- (a) Can we define an $\mathbb{R}$-linear map $f : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C}$ for which $f(z \otimes w) = z\bar{w}$?
- (b) Can we define an $\mathbb{R}$-linear map $h : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C}$ for which $h(z \otimes w) = zw$?
- (c) Can we define an $\mathbb{R}$-linear map $\ell : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C}$ for which $\ell(z \otimes w) = z + w$?

Life Tip. Suppose you want to define a linear map $g : M \otimes_R N \to P$ by very carefully defining g on every elementary tensor $m \otimes n$. Does the linearity of g follow from "additivity"? ***NO***. The map g will be linear if and only if the corresponding map $G : M \times N \to P$ defined by $G(m, n) = g(m \otimes n)$ is bilinear; so find G and check its bilinearity. Huh, how about:

(233) If $g \in \mathrm{Hom}_R(M \otimes_R N, P)$ is there a $G \in \mathrm{Bil}_R(M \times N, P)$ for which $G(m, n) = g(m \otimes n) \forall (m, n) \in M \times N$?

(234) Suppose $f : M \otimes_R N \to P$ has the property that $f(m \otimes n) = 0$ implies $m \otimes n = 0$. Is f injective? [Hint: Consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $f(z \otimes w) = z\bar{w}$.]

Life Tip. The injectivity of a linear map $f : M \otimes_R N \to P$ cannot be checked on elementary tensors (see Prompt 234.). However, if one also has a linear $g : P \to M \otimes_R N$ for which $f \circ g(p) = \mathrm{Id}_P(p)$ for all $p \in P$ and $g \circ f(t) = \mathrm{Id}_{M \otimes_R N}(t)$ for all *elementary tensors* t, then f is an isomorphism. Why?

(235) Suppose I and J are ideals in R. In Prompt (30) we showed that $I \cap J$ is the kernel of the natural map $R \to R/I \oplus R/J$. Here we establish an analogous result for $R/I \otimes_R R/J$. Can you guess what this result might say?
- (a) Recall that in Prompt (231a) we showed that every tensor in $R/I \otimes_R M$ is elementary. Show that $R/I \otimes R/J$ is a cyclic R-module with generator $\bar{1} \otimes \bar{1}$.
- (b) Use the natural function $R/I \times R/J \to R/(I + J)$ that sends $(\bar{x}, \bar{y})$ to $xy \mod I + J$ to produce a linear map $f : R/I \otimes_R R/J \to R/(I + J)$ with $f(\bar{x} \otimes \bar{y}) = \overline{xy}$.
- (c) Define a linear map $R \to R/I \otimes_R R/J$ by $r \mapsto r(\bar{1} \otimes \bar{1})$. Show that this descends to a linear map $g : R/(I + J) \to R/I \otimes_R R/J$.
- (d) Show that $f \circ g = \mathrm{Id}_{R/(I+J)}$ and $g \circ f = \mathrm{Id}_{R/I \otimes_R R/J}$.
- (e) Conclude that the map $\bar{x} \otimes \bar{y} \mapsto \overline{xy}$ induces an isomorphism $R/I \otimes_R R/J \simeq R/(I + J)$. How unique is it?
- (f) Show $R \otimes_R R \simeq R$.

Something to Think About

Given ideals I and J in R, we know how to construct the ideals $I + J$, $I \cap J$ and IJ of R. We have shown $R/I \cap J \hookrightarrow R/I \oplus R/J$ and $R/(I + J) \simeq R/I \otimes_R R/J$. What sort of object might R/IJ correspond to?

---

[1] The development here continues to follow Keith Conrad's *Tensor Products*.

[2] Sherlock Holmes never said the phrase "Elementary, my dear Watson, elementary." in any of the tales written by Arthur Conan Doyle.

Please report any errors you find to smdbackr@umich.edu

Worksheet[1] for 26 Oct 2018
Tensor products: maps, extension of scalars

Vocabulary: tensor product of maps, tensoring with N, restriction of scalars, extension of scalars, base change

Suppose R is a commutative ring. Let M, M', N, and N' be unital R modulues.

Our first goal is to understand the relationship (if any) between $\mathrm{Hom}_R(M,M')\otimes\mathrm{Hom}_R(N,N')$ and $\mathrm{Hom}_R(M\otimes_R N, M'\otimes_R N')$. We begin by looking at the latter object.

(236) Suppose $\varphi\colon \mathrm{Hom}_R(M,N)$ and $\psi\in\mathrm{Hom}_R(M',N')$.
- (a) Define $B\colon M\times M'\to N\otimes N'$ by $B(m,m')=\varphi(m)\otimes\psi(m')$. Show that this map is bilinear. Let $T(\varphi,\psi)\in\mathrm{Hom}_R(M\otimes_R M', N\otimes_R N')$ denote the corresponding linear map.
- (b) The map $T(\varphi,\psi)$ is called the *tensor product* of φ and ψ; in an (acceptable) abuse of notation, we will often denote $T(\varphi,\psi)$ by $\varphi\otimes\psi$. Why is this an abuse of notation?

Suppose $\tau\in\mathrm{Hom}_R(M,M')$. The linear maps $\mathrm{Id}_N\otimes\tau\colon N\otimes_R M\to N\otimes_R M'$ and $\tau\otimes\mathrm{Id}_N\colon M\otimes_R N\to M'\otimes_R N$ are called *tensoring with* N.

(237) Suppose $a,b\in\mathbb{Z}$. Let $\iota\colon a\mathbb{Z}\to\mathbb{Z}$ be the inclusion map. Tensoring with $\mathbb{Z}/b\mathbb{Z}$ gives a map $a\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/b\mathbb{Z}\to\mathbb{Z}/b\mathbb{Z}$. Describe the image. Conclude that "tensoring with N" need not preserve injectivity.[2]

(238) Suppose $\varphi\colon M\to M'$ is surjective. Show that $\varphi\otimes\mathrm{Id}_N\colon M\otimes_R N\to M'\otimes_R N$ is surjective. [Hint: You may want to use the result of Prompt 228a.]

As discussed in Prompt (236b) $T(\varphi,\psi)$ and $\varphi\otimes\psi$ are really very different objects – the first belongs to $\mathrm{Hom}_R(M\otimes_R N, M'\otimes_R N')$ while the second is an elementary tensor in $\mathrm{Hom}_R(M,M')\otimes\mathrm{Hom}_R(N,N')$. The next problem justifies the abuse of notation discussed in Prompt (236b).

(239) Show that there is a linear map $S\colon \mathrm{Hom}_R(M,M')\otimes_R\mathrm{Hom}_R(N,N')\to\mathrm{Hom}_R(M\otimes_R N, M'\otimes_R N')$ for which $S(\varphi\otimes\psi)=T(\varphi,\psi)$.

Suppose S is a commutative ring and $f\in\mathrm{Hom}(R,S)$ is a ring homomorphism. We now investigate an idea called "extension of scalars."

(240) Show that S is an associative[3] R-algebra where $r\in R$ acts on $s\in S$ by $r\cdot s=f(r)s$.

(241) Suppose L is a unital associative S-algebra. Show that L is an R-module where $r\cdot\ell=f(r)\ell$ for all $r\in R$ and $\ell\in L$. This means that you need to recall and verify axioms M1 through M4 in the definition of module. This process is called *restriction of scalars* and is sometimes denoted L_R or f^*L.

(242) Since M and S are both unital R-modules, we can form the R-module $S\otimes_R M$. As you will now verify, $S\otimes_R M$ has a (unique) S-module structure that, on elementary tensors, satisfies

(**) $$s\cdot(s'\otimes m)=ss'\otimes m.$$

Here $s,s'\in S$ and $m\in M$. You will also show that $r\cdot t=f(r)t$ for all tensors t in the S module $S\otimes_R M$. This process is called *extension of scalars* or *base change* and is sometimes denoted M^S or $f_!M$.
- (a) Since $S\otimes_R M$ is an R-module, module axiom M1 is free. (Why?). To define multiplication, choose $s\in S$ and consider the map
$$\mu_s\colon S\times M\to S\otimes_R M$$
defined by $\mu_s(s',m)=ss'\otimes m$. Show that μ_s is R-bilinear. Conclude that there is a multiplication map $S\times S\otimes_R M$ to $S\otimes_R M$ that sends $(s,s'\otimes m)$ to $ss'\otimes m$.
- (b) Using the scalar multiplication of S on $S\otimes_R M$ defined above, verify at least one of axioms M2 through M4 for the S-module $S\otimes_R M$. Which axiom? Ask.
- (c) Show that the S-module structure on $S\otimes_R M$ defined above satisfies $r\cdot t=f(r)t$ for all tensors $t\in S\otimes_R M$ and all $r\in R$.
- (d) *Bonus*. Show that this is the unique S-module structure on $S\otimes_R M$ satisfying (**) for elementary tensors.

(243)
- (a) Show $S\simeq S\otimes_R R$ as S-modules.
- (b) Show that, as an S-module, $S\otimes_R R^n\simeq S^n$. [Hint: You may need Homework 150.]

(244) *Bonus*. Similarly, $M\otimes_R S$ has an S-module structure given, on elementary tensors, by $s\otimes(m\otimes s')=m\otimes ss'$.

---

[1] The development here follows Keith Conrad's *Tensor Products II*.

[2] Hint: You may want to use Homework 154a to answer the injectivity question.

[3] Meaning the product operation $S\times S\to S$ is both bilinear and associative.

If $\iota\colon M \to S \otimes_R M$ is the R-homomorphism arising from tensoring $f\colon R \to S$ by M, then $M/\ker(\iota)$ is the largest quotient of M that can be embedded into any S-module (where we need to remember that the R-module structure on S is given by f).

(245) *Bonus*. Verify that the (unique) R-linear isomorphism $S \otimes_R M \simeq M \otimes_R S$ given by $s' \otimes m \mapsto m \otimes s'$ on elementary tensors is also S-linear.

(246) Show that tensoring by S has the following properties:
   (a) If $f \in \mathrm{Hom}_R(M, N)$, then $\mathrm{Id}_S \otimes f$ is an S-linear map from $S \otimes_R M$ to $S \otimes_R N$.
   (b) The identity map $\mathrm{Id}_M \in \mathrm{Hom}_R(M, M)$ goes to $\mathrm{Id}_S \otimes \mathrm{Id}_M$ which is $\mathrm{Id}_{S\otimes_R M} \in \mathrm{Hom}_S(S \otimes_R M, S \otimes_R M)$.
   (c) If $f \in \mathrm{Hom}_R(M, N)$ and $g \in \mathrm{Hom}_R(N, N')$ then $(\mathrm{Id}_S \otimes g) \circ (\mathrm{Id}_S \otimes f) = (\mathrm{Id}_S \otimes g \circ f) \in \mathrm{Hom}(S \otimes_R M, S \otimes_R N')$.

You have just verified that tensoring by S defines a functor from the category of R-modules to the category of S-modules. Is this functor faithful? is it full?

Some Things to Think About

[A] How do you think that tensoring by S interacts with direct sums? For example, should it be the case that for R-modules M_1 and M_2 we have

$$S \otimes_R (M_1 \oplus M_2) \simeq (S \otimes_R M_1) \oplus (S \otimes_R M_2)$$

as S-modules. If this is true, how unique is the isomorphism?

[B] If L is an S-module and M is an R-module, then is $M \otimes_R L$ naturally an S-modules? What is its relationship with $(S \otimes_R M) \otimes_S L$?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 29 Oct 2018
Tensor products: basic properties

Vocabulary: right exact

Suppose R is a commutative ring. Let A, B, C, and M be unital R modulues.

The notation $\oplus$ and $\otimes$ is very suggestive of addition and multiplication. We have already seen that these operations are "commutative" in the sense that $A \oplus B \simeq B \oplus A$ and $A \otimes_R B \simeq B \otimes_R A$. What about the analogues of distributivity and associativity?

(247) This problem establishes that there is a unique R-linear isomorphism $M \otimes_R (A \oplus B) \simeq (M \otimes_R A) \oplus (M \otimes_R B)$ where $m \otimes (a, b) \mapsto (m \otimes a, m \otimes b)$.
  (a) Show/Sketch that the natural map $\tau\colon M \times (A \oplus B) \to (M \otimes_R A) \oplus (M \otimes_R B)$ is bilinear.
  (b) Show/Sketch that for all bilinear maps $\beta\colon M \times (A \oplus B) \to N$ there is a unique linear map $\ell\colon (M \otimes_R A) \oplus (M \otimes_R B) \to N$ so that $\ell \circ \tau = \beta$. [Hint: To define ℓ look at $B(m, (a, 0))$ and $B(m, (0, b))$ and use the universal property of tensor products to get linear maps $M \otimes_R A \to N$ and $M \otimes_R B \to N$.]
  (c) To finish, consider the case where N is $M \otimes_R (A \oplus B)$.

The above result says that tensor products commute with direct sums. It turns out that $M \otimes_R (\oplus_{i\in I} A_i) \simeq \oplus_{i\in I}(M \otimes_R A_i)$ where I is an indexing set. **Caution.** Tensor products *do not* commute with arbitrary direct products.

(248) This problem establishes that there is a unique R-linear isomorphism $A \otimes_R (B \otimes_R C) \simeq (A \otimes_R B) \otimes_R C$ where $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$.
  (a) For uniqueness: use Prompt 228a to show that $((a \otimes b) \otimes c : (a, b, c) \in A \times B \times C)$ spans $(A \otimes B) \otimes_R C$. Similarly, show $(a \otimes (b \otimes c) \mid (a, b, c) \in A \times B \times C)$ spans $A \otimes_R (B \otimes_R C)$.
  (b) Show that for each $c \in C$ there is a unique linear map $\ell_c\colon A \otimes_R B \to A \otimes_R (B \otimes_R C)$ that maps $a \otimes b$ to $a \otimes (b \otimes c)$. [Hint: Consider the natural trilinear map $A \times B \times C \to A \otimes_R (B \otimes_R C)$. For each $c \in C$ look at the natural associated bilinear map $B_c\colon A \times B \to A \otimes_R (B \otimes_R C)$.]
  (c) Show/Sketch that the map $(A \otimes_R B) \times C \to A \otimes_R (B \otimes_R C)$ that sends (t, c) to $\ell_c(t)$ is bilinear.
  (d) Use the universal property of tensor products to produce a unique R-linear isomorphism $A \otimes_R (B \otimes_R C) \to (A \otimes_R B) \otimes_R C$ where $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$.
  (e) In a very similar fashion, construct an inverse map $(A \otimes_R B) \otimes_R C \to A \otimes_R (B \otimes_R C)$.

(249) Is every elementary tensor in $A \otimes_R (B \otimes_R C)$ of the form $a \otimes (b \otimes c)$?

Since these analogues of commutativity, associativity, and distributivity are only true "up to isomorphism", they define operations on the "set of isomorphism classes of R-modules". While we will not take it up here, pursuing these idea leads to interesting mathematics (see, e.g., Grothendieck rings).

One of the more important properties of tensoring by N is that it is *right exact*. This means that if $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact, then $A \otimes_R N \xrightarrow{\alpha\otimes \mathrm{Id}_N} B \otimes_R N \xrightarrow{\beta\otimes \mathrm{Id}_N} C \otimes_R N \to 0$ is also exact. Thanks to Prompt 237, right-exactness is the most we can hope for.

(250) Show that $\beta \otimes \mathrm{Id}_N$ is surjective. [Hint: You've already done this.]
(251) Set $I = (\alpha \otimes \mathrm{Id}_N)(A \otimes_R N)$; this is the image of $\alpha \otimes \mathrm{Id}_N$. Show that we have an inclusion of R-modules: $I \subset \ker(\beta \otimes_R \mathrm{Id}_N) \subset B \otimes_R N$. Conclude that the map $\beta \otimes \mathrm{Id}_N$ factors to a surjective R-linear map f from the cokernel $(B \otimes_R N)/I$ to $C \otimes_R N$.
(252) For $c \in C$, let $b_c \in B$ be a fixed element of $\beta^{-1}\{c\}$. Show that the assignment $(c, n) \mapsto (b_c \otimes n) + I$ produces a well defined R-bilinear map $\tilde{g}\colon C \times N \to (B \otimes_R N)/I$.
(253) Show there is an R-linear map $g\colon C \otimes_R N \to (B \otimes_R N)/I$ for which $g \circ f = \mathrm{Id}_{(B\otimes_R N)/I}$.
(254) Conclude that $I = \ker(\beta \otimes_R \mathrm{Id}_N)$. This shows that (cokernel of α) $\otimes_R N$ is the same as the cokernel of $(\alpha \otimes \mathrm{Id}_N)$.
(255) Conclude that tensoring by N is right exact.

Something to Think About

Under what conditions on N might tensoring with N also be left exact? That is, when might it happen that if $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact, then $0 \to A \otimes_R N \xrightarrow{\alpha\otimes \mathrm{Id}_N} B \otimes_R N \xrightarrow{\beta\otimes \mathrm{Id}_N} C \otimes_R N$ is also exact? Is left exactness equivalent to requiring that (kernel of α) $\otimes_R N$ is the same as the kernel of $(\alpha \otimes \mathrm{Id}_N)$?

Soon we will use ideas from homological algebra to study these questions. An R-module M for which the functor $N \mapsto N \otimes_R M$ is left exact is said to be *flat*; a term that arose from considerations in (algebraic) geometry.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 31 October 2018
Tensor product: more practice

Suppose R is a commutative ring. The point of this worksheet is to provide some additional exposure to tensor products. Some of the questions may be repeats. Do them anyway.

(256) Suppose I is an ideal in R and M is an R-module. The inclusion map $0 \to I \to R$ induces a map $I \otimes_R M \to R \otimes_R M$.
  (a) Is the induced map injective? [Justify your answer!]
  (b) Show that the image of the induced map in M is IM [Here we identify $R \otimes_R M$ with M under the natural isomorphism.]

(257) Suppose M is an R-module and I is an ideal of R. Show that $R/I \otimes_R M \simeq M/IM$

(258) Show that for all ideals I, J of R we have

$$R/I \otimes_R R/J \simeq R/(I+J).$$

(259) Compute $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ for $m, n \in \mathbb{Z}_{\geq 0}$.

(260) Show that your answer to Prompt 259 is correct in two ways: by appealing to the right exactness of tensoring and by computing it by hand.

(261) Suppose S is a PID and (r), (s) are nonzero ideals of S. What is $S/(r) \otimes_S S/(s)$?

(262) Suppose S is a PID and M, N are S-modules. Use the structure theorem for modules over a PID and Prompt 261 to describe $M \otimes_S N$.

Some problems to emphasize the role of the ring.

(263) Compute $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$. Compute $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$.

(264) Compute $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Q}/\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$.

(265) What is $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$?

(266) Show that the element represented by $2 \otimes 1$ is zero in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$ but is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$.

Some problems about basic properties of tensor products

(267) Suppose that M and N are R modules. Show that for all $m \in M$ and $n \in N$ we have $0 \otimes m = n \otimes 0 = 0$ in $N \otimes_R M$.

(268) If S is an integral domain with field of fractions K, then what is $K/S \otimes_S K/S$?

(269) Suppose I is a principal ideal in the integral domain S. Prove that the S-module $I \otimes_S I$ has no nonzero torsion elements. That is, if $0 \neq s \in S$ and $n \in I \otimes_S I$, then $sn = 0$ if and only if $n = 0$.

(270) Suppose (v, w) is a basis for $\mathbb{R}^2$. Show that $v \otimes w + w \otimes v \in \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2$ cannot be written as an elementary tensor.

(271) Suppose that F is a field and V is an F-vector space. Let $v, w \in V$. When is $v \otimes w = w \otimes v$?

Our friend $I = (2, x)$ in $S = \mathbb{Z}[x]$.

(272) Show that $\mathbb{Z}/2\mathbb{Z} \simeq S/I$. Thus $\mathbb{Z}/2\mathbb{Z}$ is an S module that is annhilated by both 2 and x.

(273) The point of this problem is to show that $2 \otimes x \neq x \otimes 2$ in $I \otimes_S I$.
  (a) Show that the map $f\colon I \times I \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$f(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0) = \frac{a_0}{2} b_1 \mod 2$$

  is S-bilinear.
  (b) Show that there is an S-module homomorphism from $I \otimes_S I$ to $\mathbb{Z}/(2)$ that maps $p(x) \otimes q(x)$ to $\frac{p(0)}{2} q'(0)$.
  (c) Conclude that $2 \otimes x \neq x \otimes 2$ in $I \otimes_S I$. (In particular, $2 \otimes x - x \otimes 2 \neq 0$.)

(274) Show that $\smiley = 2 \otimes x - x \otimes 2 \in I \otimes_S I$ is a torsion element. Compare to Prompt 269. In fact, show that both 2 and x kill $\smiley$ and the S submodule of $I \otimes_S I$ generated by $\smiley$ is isomorphic to S/I.

(275) Show that $2 \otimes 2 + x \otimes x$ is not an elementary tensor in $I \otimes_S I$. [Hint: construct a function on $I \otimes_S I$ that is zero on every elementary tensor . . .]

Something to Think About

Suppose R is a commutative ring, $D \subset R$ is multiplicative, and M is an R-module. How does $D^{-1}R$ play with $\otimes_R$? What is $M \otimes_R D^{-1}R$? If N is a $D^{-1}R$ module, what is $N \otimes_{D^{-1}R} D^{-1}M$? If R is an integral domain with field of fractions K, what sort of object is $M \otimes_R K$?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 2 Nov 2018
Tensors in the wild

If you have ever glanced at an advanced text in differential geometry or physics, then you may be wondering how the tensors we have defined in Math 593 are related to those you have encountered in the wild. We will look at this a bit here, and return to the topic in homework. The point of this worksheet is not to give an exhaustive treatment of tensors in their native habitats. Rather, the point is to help you overcome your instinct to run when you encounter them.[1]

(276) Let k be a field. Suppose V and W are finite dimensional k-vector spaces with ordered bases $\mathbf{v}$ and $\mathbf{w}$, respectively. Suppose $\dim(V) = n$ and $\dim(W) = m$. For $v \in V$ we let $[v]_{\mathbf{v}}$ denote the $n \times 1$ coordinate matrix of v with respect to $\mathbf{v}$.
   (a) For $0 \neq v \in V$ and $0 \neq w \in W$ define $A(v,w) \in \mathrm{Mat}_{n\times m}(k)$ by $A(v,w) = [v]_{\mathbf{v}}[w]_{\mathbf{w}}^T$. Show that $A(v,w)$ is a rank one matrix. (See also Prompt 231c and Prompt 223.)
   (b) Show that the nonzero elementary tensors in $V \otimes_k W$ are in bijective correspondence with the rank one matrices in $\mathrm{Mat}_{n\times m}(k)$.
   (c) Suppose $t \in V \otimes_k W$. The *rank* of t is defined to be the minimal number of pure tensors you need to add together to recover t.[2] Suppose we write $t = \sum_{i=1}^n v_i \otimes w_i$. Show that the matrix $\sum_{i=1}^n A(v_i, w_i)$ has rank k if and only if t has rank k.
   (d) Suppose $((v_i, w_i) \in V \times W \,|\, 1 \leq i \leq n)$ is a list of vectors in $V \times W$. Show that $\sum A(v_i, w_i) = 0$ if and only if for all finite dimensional vector spaces U and for all $f \in \mathrm{Bil}_k(V \times W, U)$ we have $\sum f(v_i, w_i) = 0$.
   (e) Is the map $\sum v_i \otimes w_i \mapsto \sum A(v_i, w_i)$ an isomorphism of k-vector spaces?

Being a savvy student, you noticed that the results of Prompt 276 follow easily from the far more elegant statement $V \otimes W \simeq V \otimes W^{**} \simeq \mathrm{Hom}_k(W^*, V)$ (see Homework 142). Sometimes, glossy and elegant can only be truly appreciated after tears and toil.

In physics, if $k = \mathbb{R}$ and $V = W = \mathbb{R}^n$, then for $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ the matrix $A(\mathbf{a}, \mathbf{b})$ of Prompt 231c is called a dyad[3] and is denoted $\mathbf{ab}$. Dyads are examples of what are known as "second rank[4] tensors composed of the components of two vectors" and a second rank tensor is[5] a quantity with 2 indices,[6] e.g. $A^{\mu_1\mu_2}$, whose Cartesian components $\tilde{A}^{\mu_1\mu_2}$ in a new coordinate system are obtained from the original ones by the rule

$$\tilde{A}^{\mu_1\mu_2} = \sum_{1\leq\nu_1,\nu_2\leq n} A^{\nu_1\nu_2} a_{\mu_1\nu_1} a_{\mu_2\nu_2}$$

where $(a_{\mu\nu})$ is the matrix expressing the first coordinate system of $\mathbb{R}^n$ in terms of the second.

(277) Suppose k is $\mathbb{R}$ or $\mathbb{C}$ and let V denote an n-dimensinal k-vector space. Let $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ be a basis for V. An element $D \in V^{\otimes 2} = V \otimes V$ looks like $D = \sum v_k \otimes w_k$ for $(v_k, w_k) \in V \times V$.
   (a) If we write $v_k = \sum c_{ki} e_i$ and $w_\ell = \sum b_{\ell j} e_j$, then $D = \sum_{1\leq i,j\leq n} D^{ij} e_i \otimes e_j$ where $D^{ij} = \sum_k c_{ki} b_{kj}$.

---

[1] "If you really want to impress your friends and confound your enemies, you can invoke tensor products ... People run in terror from the $\otimes$ symbol. Cool." –Brad Osgood

[2] **Warning!** The phrase "rank of a tensor" is also used in multilinear algebra where it means something completely different.

[3] A dyadic is a linear combination of dyads.

[4] **Warning!** "Rank of a tensor" is also used to describe the minimum number of pure tensors you need to add together to recover the tensor.

[5] I paraphrase from various physics textbooks.

[6] "In matters of aesthetics and mathematical notation, no one loves an index. According to one school of thought, indices are the pawns of an arcane and archaic notation, the front-line troops, the cannon fodder, first to perish in the confrontation of an inner product. Only their shadows persist. Like the putti of a Renaissance painting or the cherubim of an earlier era or, like mediaeval gargoyles, indices are mere embellishments, unnecessary appendages that adorn an otherwise bare mathematical symbol. Tensor analysis, it is claimed despite all evidence to the contrary, has nothing whatever to do with indices. 'Coordinate-free methods' and 'operator calculus' are but two of the rallying slogans for mathematicians of this persuasion. 'Computation', on the other hand, is a reactionary and subversive word. Stripped of its appendages, freed from its coordinate shackles, a plain unadorned letter is the very model of a modern mathematical operator.

Yet this extreme scorn and derision for indices is not universal. It can be argued, for example, that a 'plain unadorned letter' conceals more than it reveals. A more enlightened opinion, shared by the author, is that, for many purposes, it is the symbol itself, — that 'plain unadorned letter' — not the indices, that is the superfluous appendage. Like the grin on Alice's Cat, the indices can remain long after the symbol has gone. Just as the grin rather than the Cat is the visible display of the Cat's disposition, so too it is the indices, not the symbol, that is the visible display of the nature of the mathematical object. Surprising as it may seem, indices are capable of supporting themselves without the aid of crutches!

In matters of index notation and tensor analysis, there are few neutral observers. ..." –Peter McCullagh

(b) Suppose that $\tilde{\mathbf{e}} = (\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_n)$ is another basis for V and let $(a_{ij}) = {}_{\tilde{\mathbf{e}}}[\mathrm{Id}_V]_{\mathbf{e}}$ denote the change of basis matrix. Show that $D = \sum_{1\le i,j\le n} \tilde{D}^{ij} \tilde{e}_i \otimes \tilde{e}_j$ where $\tilde{D}^{ij} = \sum_{1\le k,\ell\le n} D^{k\ell} a_{ik} a_{j\ell}$.

(c) Conclude that D is a "second rank tensor." This shows that, in particular, dyadics are tensors in Math 593.

In differential geometry and general relativity a k-tensor on a finite dimensional real vector space V is an element of $\mathrm{Mult}(V^k, \mathbb{R})$, the vector space of multilinear functions from $V \times V \times \cdots \times V$ to $\mathbb{R}$. Thus, a 2-tensor is a bilinear map from $V \times V$ to $\mathbb{R}$; that is, it is an element of $\mathrm{Bil}_{\mathbb{R}}(V \times V, \mathbb{R})$.

(278) In this Prompt a connection between tensors in general relativity/differential geometry and tensors in Math 593 is made. This will be pursued further in homework.

(a) Show $\mathrm{Bil}_{\mathbb{R}}(V^2, \mathbb{R}) \simeq (V^{\otimes 2})^*$. [Hint: This is supposed to be easy.]

(b) Show $\mathrm{Bil}(V^2, \mathbb{R})$ is (canonically) isomorphic to $(V^*)^{\otimes 2}$. [**Warning!** This is not true if V is infinite dimensional. Homework 155b may help.]

(c) Conclude that a tensor in general relativity/differential geometry is a tensor in Math 593.

OK, back to Math 593 material.

(279) The tensor product of algebras is an algebra. Suppose R is a commutative ring and A and B are R-algebras.

(a) Suppose C is an R-module. Show that C is an R-algebra if and only if there is a linear map $m_C \in \mathrm{Hom}_R(C \otimes_R C, C)$.

(b) Show that if there is an R-algebra multiplication map on $A \otimes_R B$ satisfying $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ for all pure tensors, then it is unique.

(c) Show

$$(A \otimes_R B) \otimes_R (A \otimes_R B) \simeq ((A \otimes_R B) \otimes_R A) \otimes_R B \simeq (A \otimes_R (B \otimes_R A)) \otimes_R B \simeq (A \otimes_R (A \otimes_R B)) \otimes_R B$$
$$\simeq (A \otimes_R A) \otimes_R B) \otimes_R B \simeq (A \otimes_R A) \otimes_R (B \otimes_R B).$$

(d) Trace through what happens in the above isomorphisms to the element $(a \otimes b) \otimes (a' \otimes b')$.

(e) Compose these isomorphism with the tensor product $m_A \otimes m_B \in \mathrm{Hom}_R((A \otimes_R A) \otimes_R (B \otimes_R B), A \otimes_R B)$ where $m_A \colon A \otimes A \to A$ and $m_B \colon B \otimes_R B \to B$ are the R-linear maps corresponding to multiplication on the algebras A and B to conclude we have an R-linear map in $\mathrm{Hom}_R(A \otimes_R B) \otimes_R (A \otimes_R B), A \otimes_R B)$ that maps $(a \otimes b) \otimes (a' \otimes b')$ to $aa' \otimes bb'$.

(f) Use this R-linear map to conclude that $A \otimes_R B$ is an R-algebra.

Some things to Think About

[A] Think about the following quotes. The first is part of a response[1] by Kim Aaron to the question "What is the physical meaning of a tensor?"

> A tensor is a description about what happens in one direction due to what's happening in other directions.

The second is part of a response[2] by Warren Davis to the question "What is a tensor?"

> An example of a second order[3] tensor is the so-called inertia matrix (or tensor) of an object. For three dimensional objects, it is a $3 \times 3 = 9$ element array that characterizes the behavior of a rotating body. As is well known to anyone who has played with a toy gyroscope, the response of a gyroscope to a force along a particular direction (described by a vector), is generally re-orientation along some other direction different from that of the applied force or torque. Thus, rotation must be characterized by a mathematical entity more complex than either a scalar or a vector; namely, a tensor of order two.

[B] Tensors arise in quantum mechanics – one is looking at the (completed) tensor product of Hilbert spaces. I couldn't find something in this direction that was both concise and interesting; if you have an idea, please let me know.

[C] For more examples of tensors in the wild, see Peter McCullagh's book *Tensor Methods in Statistics*.[4]

---

[1] www.quora.com/What-is-the-physical-meaning-of-a-tensor-What-are-interesting-examples-of-tensors-in-phy

[2] http://www.physlink.com/Education/AskExperts/ae168.cfm

[3] i.e., rank two

[4] Available at http://www.stat.uchicago.edu/~pmcc/tensorbook/. I particularly like the introductory passage titled "Difficult Questions."

Please report any errors you find to smdbackr@umich.edu

Worksheet for 5 Nov 2018
Higher tensors, symmetric and alternating maps

Vocabulary: multilinear maps, multilinear form, skew-symmetric maps, symmetric maps, alternating maps, higher tensor products, d^{th} exterior power module, 2^{nd} symmetric power module,

Suppose R is a commutative ring. Let M, M_1, M_2, …, and P be unital R modules. We will freely use the fact that products and tensor products are associative operations.

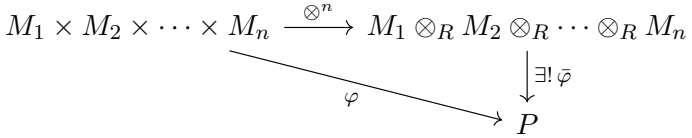
Definition. Suppose $f\colon M_1 \times M_2 \times \cdots \times M_{n-1} \times M_n \to P$ is a function. The function f is called *R-multilinear* provided that it is R-linear in each variable (for fixed values of the remaining variables).

(280) Show that $f(X,Y,Z) = XYZ - YXZ - XZY + YZX - ZYX + ZXY$ is a multilinear function from $\mathrm{Mat}_{\ell\times\ell}(R) \times \mathrm{Mat}_{\ell\times\ell}(R) \times \mathrm{Mat}_{\ell\times\ell}(R)$ to $\mathrm{Mat}_{\ell\times\ell}(R)$.

(281) Show that the set of multilinear maps from $M_1 \times M_2 \times \cdots \times M_{n-1} \times M_n$ to P has a natural R-module structure.

Just as bilinear functions were the key to defining tensor products, multilinear functions are the key to defining *higher tensor products*. A straightforward induction argument (do you see it?) shows that every R-multilinear map $M_1 \times M_2 \times \cdots \times M_n \to P$ factors uniquely through an R-linear map $((\cdots(M_1 \otimes_R M_2) \otimes_R M_3)\otimes)\cdots) \otimes_R M_n) \to P$. Thus:

Universal Property of higher tensor products. The *tensor product* $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n$ is an R-module with a multilinear map $\otimes^n\colon M_1 \times M_2 \times \cdots \times M_n \to M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n$ such that for every R-multilinear map $\varphi\colon M_1 \times M_2 \times \cdots \times M_n \to P$ there is a unique linear map $\bar\varphi \in \mathrm{Hom}_R(M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n, P)$ for which the following diagram commutes.

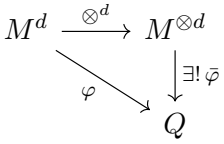


(282) Show there is a bijective correspondence between the R-module of multilinear maps from $M_1 \times M_2 \times \cdots \times M_{n-1} \times M_n$ to P and $\mathrm{Hom}_R(M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n, P)$.

Definition. Set $M^d = M \times M \times \cdots \times M$ and $M^{\otimes d} = M \otimes_R M \otimes_R \cdots \otimes_R M$ (there are d copies of M on the RHS of both of these expressions). The space of R-multilinear functions $f\colon M^d \to P$ is denoted $\mathrm{Mult}^d_R(M,P)$.

The R-module $M^{\otimes d}$ is often denoted $T^d(M)$. An R-multilinear function with values in R is often called an *R-multilinear form*.

Thanks to our work above, for every R-module Q and every $\varphi \in \mathrm{Mult}^d_R(M,Q)$ there is a unique $\bar\varphi \in \mathrm{Hom}_R(M^{\otimes d}, Q)$ for which the following diagram commutes.



There are two natural submodules of $\mathrm{Mult}^d_R(M,P)$ that are ubiquitous in mathematics:

Definition. A function $f \in \mathrm{Mult}^d_R(M,P)$ is called *alternating* provided that $f(m_1, m_2, \ldots, m_d) = 0$ whenever there exists $i \neq j$ such that $m_i = m_j$. It is called *symmetric* provided that

$$f(m_1, m_2, \ldots, m_d) = f(m_{\sigma(1)}, m_{\sigma(2)}, \ldots, m_{\sigma(d)})$$

for all $\sigma \in S_d$, the symmetric group on d letters.
The R-submodule of $\mathrm{Mult}^d_R(M,P)$ consisting of alternating functions is denoted $\mathrm{Alt}^d_R(M,P)$ and the R-submodule of $\mathrm{Mult}^d_R(M,P)$ consisting of symmetric functions is denoted $\mathrm{Sym}^d_R(M,P)$.

(283) Show that if $2 \in R^\times$, then $f \in \mathrm{Mult}^d_R(M,P)$ is alternating if and only if it is skew-symmetric (i.e., switching two entries results in a change of sign). Conclude that

$$f(m_{\sigma(1)}, m_{\sigma(2)}, \ldots, m_{\sigma(d)}) = \mathrm{sgn}(\sigma) f(m_1, m_2, \ldots, m_d)$$

for all $\sigma \in S_d$. What can you say when $2 \notin R^\times$?

(284) Suppose k is a field. Show that the map $(\vec{v}, \vec{w}) \mapsto \vec{v}^T\vec{w}$ (aka the dot product) defines an element of $\mathrm{Sym}^2_k(k^n, k)$

(285) Suppose $f \in \mathrm{Mult}^d_R(M, P)$. Reformulate the condition for f to belong to the submodule $\mathrm{Sym}^d_R(M)$ in terms of transpositions (aka involutions on $\{1, 2, 3, \ldots, d\}$).

(286) Show that the function f defined in Prompt 280 belongs to $\mathrm{Alt}^3_R(\mathrm{Mat}_{\ell\times\ell}(R), \mathrm{Mat}_{\ell\times\ell}(R))$.

Just as $\mathrm{Mult}^d_R(M, \cdot)$ corresponds to the universal object $M^{\otimes d} = T^d(M)$, so too $\mathrm{Alt}^d_R(M, \cdot)$ and $\mathrm{Sym}^d_R(M, \cdot)$ have their corresponding universal objects.

For example, every function in $\mathrm{Alt}^d_R(M, \cdot)$ is multilinear and vanishes on d-tuples that have two equal entries. Thus, we should consider the R-submodule $X = \langle m_1 \otimes m_2 \otimes \cdots \otimes m_d \,|\, m_i = m_j \text{ for some } i \neq j\rangle$ of $M^{\otimes d}$ and our candidate universal object is the quotient module $\bigwedge^d_R(M) = M^{\otimes d}/X$, which is called the *$d^{th}$ wedge power module* or *d^{th} exterior power module*. The induced map

$$\wedge^d \colon M^d \xrightarrow{\otimes^d} M^{\otimes d} \longrightarrow \bigwedge^d_R(M)$$

is alternating,[1] and the image of $(m_1, m_2, \ldots, m_d) \in M^d$ under this map is denoted $m_1 \wedge m_2 \wedge \cdots \wedge m_d$, which is sometimes called a *pure wedge* in analogy with pure tensors.

(287) Show that for all R-modules Q and all $f \in \mathrm{Alt}^2_R(M, Q)$ there exists a unique $\bar{f} \in \mathrm{Hom}_R(\bigwedge^2_R(M), Q)$ for which the following diagram commutes. (You will consider the general case in Homework 187.)

$$\begin{array}{ccc} M \times M & \xrightarrow{\wedge^2} & (M \otimes_R M)/\langle m \otimes m\rangle \\ & \searrow^{f} & \downarrow \bar{f} \\ & & Q \end{array}$$

(288) Show that for all R-modules Q and all $f \in \mathrm{Sym}^2_R(M, Q)$ there exists a unique $\bar{f} \in \mathrm{Hom}_R((M \otimes_R M)/\langle m_1 \otimes m_2 - m_2 \otimes m_1\rangle, Q)$ for which the following diagram commutes. (You will consider the general case in Homework 188.)

$$\begin{array}{ccccc} M \times M & \xrightarrow{\otimes^2} & M \otimes M & \longrightarrow & (M \otimes_R M)/\langle m_1 \otimes m_2 - m_2 \otimes m_1\rangle \\ & \searrow^{f} & & & \downarrow \bar{f} \\ & & & & Q \end{array}$$

The quotient module $S^2_R(M) = (M \otimes_R M)/\langle m_1 \otimes m2 - m_2 \otimes m_1\rangle$ is called the *2^{nd} symmetric power module*.

Something to Think About

Given $f \in \mathrm{Mult}^k_R(M, R)$ and $g \in \mathrm{Mult}^\ell_R(M, R)$, we can form an element of $\mathrm{Mult}^{k+\ell}_R(M, R)$ by sending $(m_1, m_2, \ldots m_k, m_{k+1}, \ldots, m_{k+\ell})$ to $f(m_2, m_2, \ldots, m_k)g(m_{k+1}, m_{k+2}, \ldots, m_{k+\ell})$. This suggests that we have maps $\otimes \colon M^{\otimes k} \times M^{\otimes \ell} \to M^{\otimes(k+\ell)}$, $\wedge \colon \bigwedge^k(M) \times \bigwedge^\ell(M) \to \bigwedge^{k+\ell}(M)$, and $\cdot \colon S^k(M) \times S^\ell(M) \to S^{k+\ell}(M)$. Can you define such maps? Even stronger, it suggests that perhaps we should set $M^{\otimes 0} := R$, $M^{\otimes 1} = M$, and study the *graded R-module*

$$T(M) = \bigoplus_{d\geq 0} M^{\otimes d} = R \oplus M \oplus M^{\otimes 2} \oplus M^{\oplus 3} \oplus \cdots$$

This turns out to be a very useful way to view things. How would you define $\bigwedge(M)$ or $S(M)$ as a quotient of $T(M)$? Would you be able to recover $\bigwedge^d(M)$ as the "degree d piece of $\bigwedge(M)$" or $S^d(M)$ as the "degree d piece of $S(M)$"?

[1] Note that X is the smallest submodule of $M^{\otimes d}$ for which the induced map from M^d to $M^{\otimes d}/X$ is alternating.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 7 Nov 2018
Bilinear forms

Vocabulary: bilinear form, symmetric, alternating, skew-symmetric, anti-symmetric, rank, nondegenerate, cogredient, congruent

Bilinear forms appear in pretty much every part of mathematics: in Euclidean geometry one sees the dot product, in relativity theory one sees the Minkowski inner product, in the study of Lie algebras and Lie groups one sees the Killing form, in Math 593 bilinear forms are everywhere, ...

Suppose k is a field and V is a k-vector space.

Definition. A *k-bilinear form on V* is an element of $\mathrm{Bil}(V \times V, k)$. A k-bilinear form B on V is said to be

- *symmetric* provided that $B(x, y) = B(y, x)$ for all $x, y \in V$,
- *alternating* provided that $B(u, u) = 0$ for all $u \in V$, and
- *skew-symmetric* (or *anti-symmetric* provided that $B(s, t) = -B(t, s)$ for all $s, t \in V$.

(289) For $v, w \in \mathbb{R}^2$, let $v \cdot w$ denote the usual dot product (which is really just $v^T w$). Suppose $A \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$ and set $B_A(x, y) = x \cdot (Ay)$. B_A will serve as a template for understanding bilinear forms in the finite dimensional case.
  (a) Show that $B_A \in \mathrm{Bil}(\mathbb{R}^2 \times \mathbb{R}^2, \mathbb{R})$.
  (b) Under what conditions will B_A be symmetric? [Hint: Do some calculations with respect to a basis.]
  (c) Under what conditions will B_A be alternating?
  (d) Under what conditions will B_A be skew-symmetric?

If things went well, your answers to Prompts 289c and 289d were the same; these will be generalized in Homework 180. The agreement between alternating and skew-symmetry almost always holds (for vector spaces). However, bilinear forms over characteristic two fields usually require special care. Depending on your perspective, this "special care" is either cool or a headache.[1]

(290) Show that every alternating form is skew symmetric. [Hint: A standard trick in bilinear form calculuations is to look at $B(u + v, u + v)$.]
(291) Show that when the characteristic of k is not two we have that every skew-symmetric form is alternating.
(292) Note that in characteristic two alternating $\Rightarrow$ skew-symmetric $\Leftrightarrow$ symmetric. In characteristic two can you produce a symmetric bilinear form that is not alternating?

The involution $f \in \mathrm{Hom}_k(V^2, V^2)$ that takes (v, v') to (v', v) induces an action on the k-vector space $\mathrm{Bil}(V^2, k)$.

(293) When k is not of characteristic two, we have $\mathrm{Bil}(V^2, k) = \mathrm{Bil}(V^2, k)(1) \oplus \mathrm{Bil}(V^2, k)(-1)$. [Hint: Look at $B + B \circ f$ and $B - B \circ f$. Why do we need to assume that the characteristic of k is not two?]
(294) Conclude that every $B \in \mathrm{Bil}(V^2, k)$ can be decomposed as $B = S + A$ where $S, A \in \mathrm{Bil}(V^2, k)$ with S symmetric and A alternating. How is this related to Homework 147?

Suppose now that V is finite dimensional and that $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is a basis of V. Recall that for $y \in V$ we write the coordinates of y with respect to $\mathbf{v}$ as $[y]_{\mathbf{v}}$. Here $[y]_{\mathbf{v}} = [y_1, y_2, \ldots, y_n]^T$ if and only if $y = \sum y_i v_i$.

(295) Suppose $B \in \mathrm{Bil}(V^2, k)$. Define $M = M(B, \mathbf{v}) \in \mathrm{Mat}_{n\times n}(k)$ by setting $M_{ij} = B(v_i, v_j)$. Show that $B(x, y) = [x]_{\mathbf{v}}^T M [y]_{\mathbf{v}}$.
(296) Suppose $A \in \mathrm{Mat}_{n\times n}(k)$. Define $B_A(x, y) = [x]_{\mathbf{v}}^T A [y]_{\mathbf{v}}$. Show that $B_A \in \mathrm{Bil}(V^2, k)$.
(297) Show that $B \mapsto M(B, \mathbf{v})$ from $\mathrm{Bil}(V^2, k)$ to $\mathrm{Mat}_{n\times n}(k)$ is an isomorphism of k-vector spaces.

Warning: The k-algebra isomorphism $\mathrm{End}_k(V) \simeq \mathrm{Mat}_{n\times n}(k)$ given by $T \mapsto_{\mathbf{v}} [T]_{\mathbf{v}}$ (see Homework 108) is a completely different beast than the k-module isomorphism $B \mapsto M(B, \mathbf{v})$. In particular, while we can add and scalar multiply bilinear forms, there is no natural way to define the composition of bilinear forms on V.

However, we can make use of the k-module isomorphism $B \mapsto M(B, \mathbf{v})$ to think about what the rank, determinant, trace, etc. of $M(B, \mathbf{v})$ might mean for B. Our first order of business is to figure out if there is any relationship between $M(B, \mathbf{v})$ and $M(B, \tilde{\mathbf{v}})$ where $\tilde{\mathbf{v}}$ is another basis for V.

(298) Let $Q =_{\tilde{\mathbf{v}}} [\mathrm{Id}_V]_{\mathbf{v}}$ and fix $B \in \mathrm{Bil}(V^2, k)$.
  (a) Show that Q is invertible.

[1] To see another reason why, depending on your perspective, two may turn out to be cool or a headache, check out the graph of A000001, the number of groups of order n, at The On-line Encyclopedia of Integer Sequences. oeis.org/A000001/graph.

(b) Show that $M = Q^T \tilde{M} Q$. where $M = M(B, \mathbf{v})$ and $\tilde{M} = M(B, \tilde{\mathbf{v}})$. (The matrices M and $\tilde{M}$ are said to be *cogredient* or *congruent*, cogrediency is an equivalence relation.)

(c) Show that for all $T \in \mathrm{End}_k(V)$ we have ${}_{\mathbf{v}}[T]_{\mathbf{v}} = Q^{-1}{}_{\tilde{\mathbf{v}}}[T]_{\tilde{\mathbf{v}}} Q$.

Thanks to Prompt 298b and Homeworks 164a and 164b the following defintion makes sense.

Definition. Fix a basis $\mathbf{v}$ of V and a bilinear form $B \in \mathrm{Bil}(V \times V, k)$. B is said to be *nondegenerate* provided that $\det(M(B, \mathbf{v})) \neq 0$. The *rank* of B is defined to be the rank of $M(B, \mathbf{v})$.

Thanks to Prompts 289c and 289d (along with Homework 180) we know that the map $B \mapsto M(B, \mathbf{v})$ should take symmetric bilinear forms to *symmetric matrices* (those for which $A = A^T$), skew-symmetric bilinear forms to *skew-symmetric matrices* (those for which $A = -A^T$), and alternating forms to skew-symmetric matrices all of whose diagonal entries are zero. It is comforting that in the change of coordinates expression of Prompt 298b we see that if $\tilde{M}$ is symmetric then so too is M. Similarly, if one of $\tilde{M}$ or M is skew-symmetric, then so too is the other. If one of them has all diagonal entries does the other?

Something to Think About

It should trouble your soul that the map $B \mapsto M(B, \mathbf{v})$ involves a choice – why are we favoring the "right" variable? Why not favor the left and define $B_A(x, y) = (A[x]_{\mathbf{v}})^T [y]_{\mathbf{v}}$? Does this choice make a difference? How to account for it?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 9 Nov 2018
Symmetric bilinear forms

Vocabulary: Sylvester's Law of Inertia, signature, quadratic form

Suppose k is a field not of charactersitc two. In Homework 143 EROs and ECOs were used to show that if $A \in \mathrm{Mat}_{n\times n}(k)$ is a symmetric matrix, then there exists invertible $Q \in \mathrm{Mat}_{n\times n}(k)^\times$ so that $Q^T AQ$ is diagonal. In terms of bilinear forms on a finite dimensional vector space V, this means that if $B \in \mathrm{Bil}(V^2, k)$ is a symmetric bilinear form on V, then

(*) there is a basis $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ of V for which $M(B, \mathbf{v})$ is diagonal;

that is, $B(v_i, v_j) = b_i\delta_{ij}$ for some $b_i \in k$. Because it helps motivate some later ideas, let's prove this result again.[1]

(299) Show that if $B \neq 0$, then there exists $x \in V$ for which $B(x, x) \neq 0$. [Hint: Consider $B(u+v, u+v) - B(u, u) - B(v, v)$.]

(300) Suppose we can choose $u_1, u_2, \ldots, u_k \in V$ for which $B(u_i, u_j) = b_i\delta_{ij}$ with $b_i \neq 0$. Let $V_k = \mathrm{span}(u_1, u_2, \ldots, u_k)$. Set $V_k^\perp = \{w \in V \mid B(v, w) = 0 \text{ for all } v \in V_k\}$.
  (a) Show that $V_k \cap V_k^\perp = \{0\}$.
  (b) Suppose $y \in V$. Show that

$$x = y - \sum_{i=1}^{k} B(u_i, y) b_i^{-1} u_i$$

  belongs to $V_k^\perp$.
  (c) Conclude that $V = V_k \oplus V_k^\perp$. (Here we are forming an "internal direct sum.")

(301) Show that Property (*) holds. [If $B = 0$, then any basis will satisfy Property (*), so there is nothing to prove. Let us assume $B \neq 0 \ldots$]

Warning: From Homework 143 we know that Property (*) need not hold when k has characteristic two.

Since a basis $\mathbf{v}$ can be chosen so that $M(B, \mathbf{v})$ is diagonal, it is natural to ask: how unique are the diagonal entries of $M(B, \mathbf{v})$ – that is, can we find a way to classify all elements of $\mathrm{Bil}(V^2, k)$ in terms of n-tuples? This turns out to be an extremely interesting question. It follows from Prompt 298b that we could hope that the diagonal entries of $M(B, \mathbf{v})$ are, up to rearrangement, uniquely determined modulo $(k^\times)^2$ – that is, we could hope that the elements of $\mathrm{Bil}(V^2, k)$ are determined by n-tuples of elements of $k^\times/(k^\times)^2$. However, Homework 143c shows that this doesn't work already for $\mathrm{Bil}(\mathbb{Q}^2 \times \mathbb{Q}^2, \mathbb{Q})$.

In special situations, like k finite or k algebraically closed, one can parameterize the bilinear forms up to cogrediency (see [J85, §6.3]). For ordered fields, we have the following result.

(302) (Sylvester's Law of Inertia) Suppose that k is an ordered field.[2] Suppose $B \in \mathrm{Bil}(V^2, k)$ and there exist bases $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\tilde{\mathbf{u}} = (\tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_n)$ so that

$$M(B, \mathbf{u}) = \mathrm{diag}(m_1, m_2, \ldots, m_r, 0, 0, \ldots, 0)$$

with $m_1, m_2, \ldots, m_p$ positive and $m_{p+1}, m_{p+2}, \ldots, m_r$ negative and

$$M(B, \tilde{\mathbf{u}}) = \mathrm{diag}(\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_{\tilde{r}}, 0, 0, \ldots, 0)$$

with $\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_{\tilde{p}}$ positive and $\tilde{m}_{\tilde{p}+1}, m_{\tilde{p}+2}, \ldots, m_{\tilde{r}}$ negative.
  (a) Show that $r = \tilde{r}$. [Hint: See Homework 164a]
  (b) Consider $x \in V^+ = \mathrm{span}(u_1, u_2, \ldots, u_p)$. Show that $B(x, x) \geq 0$ with equality if and only if $x = 0$.
  (c) Consider $y \in V^- = \mathrm{span}(\tilde{u}_{\tilde{p}+1}, \tilde{u}_{\tilde{p}+2}, \ldots, \tilde{u}_n)$. Show that $B(y, y) \leq 0$.
  (d) Since $V^+ \cap V^- = \{0\}$ (why?), conclude that $p \leq \tilde{p}$. [Hint: $\dim(V^+ + V^-) = \dim(V^+) + \dim(V^-) - \dim(V^+ \cap V^-)$ – why?]

[1] The following proof is due to Lagrange.

[2] We say that a field k is ordered provided that: (a) if $x, y \in k_{>0}$, then $xy > 0$ and $x + y > 0$; and (b) if $z \in k$ then exactly one of the following is true: (i) $z > 0$, (ii) $z = 0$, or (iii) $z < 0$. Wait, what does the symbol $>$ mean?

Please report any errors you find to smdbackr@umich.edu

Thanks to Prompt 302, the following definition makes sense.

Definition. Suppose k is an ordered field, V is an n dimensional k-vector space, and $B \in \mathrm{Bil}(V \times V, \mathbb{R})$. Choose a basis $\mathbf{u}$ of V such that $M(B, \mathbf{u})$ is diagonal. Let n_+ denote the number of positive entries on the diagonal of $M(B, \mathbf{u})$, and let n_- denote the number of negative entries on the diagonal of $M(B, \mathbf{u})$. The difference $(n_+ - n_-)$ is called the *signature* of B. [Some people call the triple $((n - (n_+ + n_-), n_+, n_-, (n - (n_+ + n_-))$ the *signature* of B.]

Note that $(n_+ + n_-)$ is the rank of B.

(303) Suppose V is an n dimensional real vector space and $B \in \mathrm{Bil}(V \times V, \mathbb{R})$. Suppose the rank of B is k and its signature is ℓ. Show there exists a basis $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ of V such that

$$M(B, \mathbf{u}) = \mathrm{diag}(1, 1, \ldots, 1, -1, -1, \ldots, -1, 0, 0, \ldots 0)$$

with $(k + \ell)/2$ ones, $(k - \ell)/2$ minus ones, and $n - k$ zeros.

Definition. A *quadratic form* on V is a map $Q \colon V \to k$ for which

(1) $Q(ax) = a^2 Q(x)$ for all $a \in k$ and $x \in V$, and
(2) the function $(x, y) \mapsto B_Q(x, y) := Q(x + y) - Q(x) - Q(y)$. belongs to $\mathrm{Bil}(V^2, k)$.

(304) Show that if $B \in \mathrm{Bil}(V^2, k)$, then $Q_B(x) = B(x, x)$ is a quadratic form on V. What is the relationship between Q_B and B_Q? Is the theory of quadratic forms the same as that of symmetric binary forms (when the characteristic of k is not two)?

Something to Think About

The classification of quadratic forms/symmetric bilinear forms is often very challenging. The solution for $k = \mathbb{Q}$ is quite beautiful and is known as the Hasse-Minkowski theorem. This theorem says that two bilinear forms B and B' in $\mathrm{Bil}(V^2, \mathbb{Q})$ are equivalent if and only if they are equivalent in $\mathrm{Bil}((V \otimes_{\mathbb{Q}} \mathbb{R})^2, \mathbb{R})$ and $\mathrm{Bil}((V \otimes_{\mathbb{Q}} \mathbb{Q}_p)^2, \mathbb{Q}_p)$ for all primes p. This is an example of putting to good use a philosophy known as the *local-global principle* or *Hasse principle* which states that we can often understand/solve/make progress on a problem over $\mathbb{Q}$ by understanding/solving/making progress on it over every completion of $\mathbb{Q}$ (that is, $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p). Can you think of other problems to which the local-global principle might apply?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 12 Nov 2018
Inner products

Vocabulary: complex conjugate, inner product, conjugate linear, symmetric sesquilinear form, Hermitian form, inner product space, orthogonal complement, normal

Throughout this worksheet k is either the field of real numbers, $\mathbb{R}$, or the field of complex numbers, $\mathbb{C}$. If $z \in \mathbb{C}$, then we denote by $\overline{z}$ the *complex conjugate* of z and set $|z| = \sqrt{z\overline{z}}$, this is sometimes called the *modulus* of z. In Cartesian form we have $\overline{a+ib} = a - ib$ and in polar form we have $\overline{re^{i\theta}} = re^{-i\theta}$. (Note that $r = \left|re^{i\theta}\right|$.) Complex conjugation is an involution on $\mathbb{C}$, and the set of fixed points of this involution is the field $\mathbb{R}$.

Definition. Suppose k is either $\mathbb{R}$ or $\mathbb{C}$ and let V be a k-vector space. An *inner product* on V is a function $\langle\ ,\ \rangle \colon V \times V \to k$ that satisfies

(1) For all $u, w, v \in V$ we have $\langle u+v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$.
(2) For all $u, w \in V$ and $a \in k$ we have $\langle au, w\rangle = a\langle u, w\rangle$.
(3) For all $u, w \in V$ we have $\langle u, w\rangle = \overline{\langle w, u\rangle}$.
(4) for all $v \in V$ we have $\langle v, v\rangle \geq 0$ with equality if and only if $v = 0$.

In words: an inner product is a bi-addivive function from $V \times V$ to k which is linear in the first term, conjugate symmetric, and positive definite.

(305) Show that if V is an $\mathbb{R}$-vector space, then an inner product on V is a symmetric bilinear form.

(306) Suppose V is a $\mathbb{C}$-vector space and $\langle\ ,\ \rangle$ is an inner product on V. Show that for all $u, v, w \in V$ and $c \in \mathbb{C}$ we have $\langle w, u + cv\rangle = \langle w, u\rangle + \overline{c}\langle w, v\rangle$. In particular, an inner product is **not** a bilinear form since it is linear in the first variable and *conjugate linear* in the second.[1]

Since an inner product over $\mathbb{C}$ is not bilinear, it is sometimes called a *symmetric sesquilinear form* or *Hermitian form* to remind us that it is not bilinear.

(307) Suppose V is a finite dimensional k-vector space. Let $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be a basis for V. For $x, y \in V$ define $\langle x, y\rangle = \sum_i x_i\overline{y_i}$ where $x = \sum x_k v_k$ and $y = \sum y_j v_j$. Show this defines an inner product on V.

(308) Let $C^0([0,1], k)$ denote the k-vector space of k-valued continuous function on $[0,1]$. For $f, g \in C^0([0,1])$ set $\langle f, g\rangle = \int_0^1 f(x)\overline{g(x)}\,dx$. Show this defines an inner product on $C^0([0,1], k)$.

Definition. An *inner product space* is a real or complex vector space, together with a specified inner product on that space.

Note that in the Homework b problems, we have been restricting ourselves to real inner product spaces.

Definition. Suppose V is an inner product space with inner product $\langle\ ,\ \rangle$. For $v \in V$ define the *norm* of v, denoted $\|v\|$, by $\|v\| = \sqrt{\langle v, v\rangle}$. A nonzero list of vectors $(u_1, u_2, \ldots, u_m)$ in V is said to be *orthogonal* provided that $\langle u_i, u_j\rangle = 0$ for all $1 \leq i \neq j \leq m$ and it is said to be *orthonormal* provided that it is an orthogonal list with $\|u_k\| = 1$ for all $1 \leq k \leq m$. Finally, if W is a subspace of V, then the *orthogonal complement to W in V* is $W^\perp = \{v \in V \mid \langle v, w\rangle = 0 \text{ for all } w \in W\}$.

In Homework 198 it will be shown that $W + W^\perp = V$ and $W \cap W^\perp = \{0\}$.

Suppose V is an inner product space and $T \in \mathrm{Hom}_k(V, V)$. It is natural to ask: when does there exist an orthonormal eigenbasis for V? That is, when can we find an orthonormal basis $(u_1, u_2, \ldots)$ for V so that $T(u_j) = \alpha_j u_j$ for $\alpha_j \in k$ and all indices j? We explore this question for the case when V is finite-dimensional. Suppose V has dimension n.

Exactly as in Homeworks 131d and 131e we can define the adjoint, $T^* \in \mathrm{Hom}_k(V, V)$, of T by requiring that $\langle T(v), w\rangle = \langle v, T^*(w)\rangle$ for all $v, w \in V$. Note that $T^{**} = T$.

(309) Suppose $T \in \mathrm{Hom}_k(V, V)$. Suppose that W is a subspace of V that is T invariant. Show that $W^\perp$ is T^*-invariant.

(310) Suppose $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is an orthonormal basis for V. Show that ${}_{\mathbf{v}}[T^*]_{\mathbf{v}}$ is the conjugate transpose of ${}_{\mathbf{v}}[T]_{\mathbf{v}}$. That is, if a_{ij} denotes the entry in the ith row and jth column of ${}_{\mathbf{v}}[T]_{\mathbf{v}}$, then the entry in the kth row and ℓth column of ${}_{\mathbf{v}}[T^*]_{\mathbf{v}}$ is $\overline{a_{\ell k}}$. Do we need to assume that the basis $\mathbf{v}$ is orthonormal?

(311) Conclude that if T admits an orthonormal basis $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ for V so that $T(u_j) = \alpha_j u_j$ for $\alpha_j \in k$, then ${}_{\mathbf{u}}[T]_{\mathbf{u}} = \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and ${}_{\mathbf{u}}[T^*]_{\mathbf{u}} = \mathrm{diag}(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n)$.

[1] Some people do things in the opposite order – their inner products over $\mathbb{C}$ are linear in the second variable and conjugate linear in the first variable; this leads to much confusion.

Please report any errors you find to smdbackr@umich.edu

Thanks to Prompt 311 if $k = \mathbb{R}$ and T admits an orthonormal eigenbasis, then since all eigenvalues are in $\mathbb{R}$, we conclude that T is self-adjoint (that is, $T = T^*$). As you will show in Homework 210, the converse is also true: if $k = \mathbb{R}$ and $T = T^*$, then T admits an orthonormal eigenbasis.

What if $k = \mathbb{C}$? In this case, it seems that all we can conclude is that T and T^* commute; that is $T \circ T^* = T^* \circ T$. While this condition doesn't appear to be very strong, it turns out that it is sufficient.[1]

Definition. Suppose V is finite-dimensional inner product space. A linear transformation $T \in \mathrm{Hom}_k(V, V)$ is said to be *normal* provided that $T \circ T^* = T^* \circ T$.

We the remainder of this worksheet we assume that V is a finite dimensional inner product space.

(312) *Bonus.* Show that $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ is normal if and only if $T = R + iS$ with R and S self adjoint.

(313) Suppose $N \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ is normal.
- (a) Show that $\|N(v)\| = \|N^*(v)\|$ for all $v \in V$.
- (b) Show that $N - c\,\mathrm{Id}_V$ is normal for all $c \in \mathbb{C}$.
- (c) Show that if v is an eigenvector for N with eigenvalue α, then v is an eigenvalue of N^* with eigenvalue $\overline{\alpha}$.

(314) Suppose $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ with $V \neq \{0\}$. Show that T admits an eigenvector v with $\|v\| = 1$.

(315) Suppose $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ is normal and $V \neq \{0\}$. Let u be a norm one eigenvector for T.
- (a) Let $U = \mathrm{span}_{\mathbb{C}}(u)$. Use Prompt 313 to show that both T and T^* preserve both U and $U^{\perp}$.
- (b) Show that the restriction of T to $U^{\perp}$ is normal.

(316) (Spectral Theorem for Normal Operators) Conclude: If $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ is normal, then T admits an orthonormal eigenbasis. [Hint: If $V = \{0\}$, there is nothing to prove. If $\dim_{\mathbb{C}}(V) = 1$, then ....]

Some things to Think About

[A] Suppose V is a finite-dimensional inner product space over $\mathbb{C}$ with inner product $\langle\ ,\ \rangle$. Even though $\langle\ ,\ \rangle$ is not bilinear, it turns out that just as for bilinear forms when given an orthogonal basis $\mathbf{v}$ of V one can produce a conjugate symmetric matrix $M(\mathbf{v})$ so that

$$\langle x, y\rangle = [x]_{\mathbf{v}}^T\, M(\mathbf{v})\, \overline{[y]}_{\mathbf{v}}.$$

Since a conjugate symmetric matrix is normal (why?), we can find an orthogonal basis $\mathbf{u}$ so that $M(\mathbf{u})$ is diagonal. Can we find a basis $\mathbf{w}$ so that $M(\mathbf{w})$ is the identity? How are these bases related?

[B] There are many important generalizations of the spectral theorem. Some, like the Singular Value Decomposition, play a very important role in applied mathematics. Others, like the Spectral Theorem for Compact Self-adjoint Operators, play an important role in functional analysis and representation theory. Why are theorems like the spectral theorem uselful/important?

[1] This condition is stronger than it appears. Here is a way to think about it: in Homework 163 we saw that over $\mathbb{R}$ the condition $S \circ S^* = S^* \circ S = \mathrm{Id}_V$ means that S must be an orthogonal transformation. The condition that T and T^* commute is a 'small' relaxation of this requirement.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 16 Nov 2018
The Snake Lemma

Vocabulary: snake lemma, connecting homomorphism

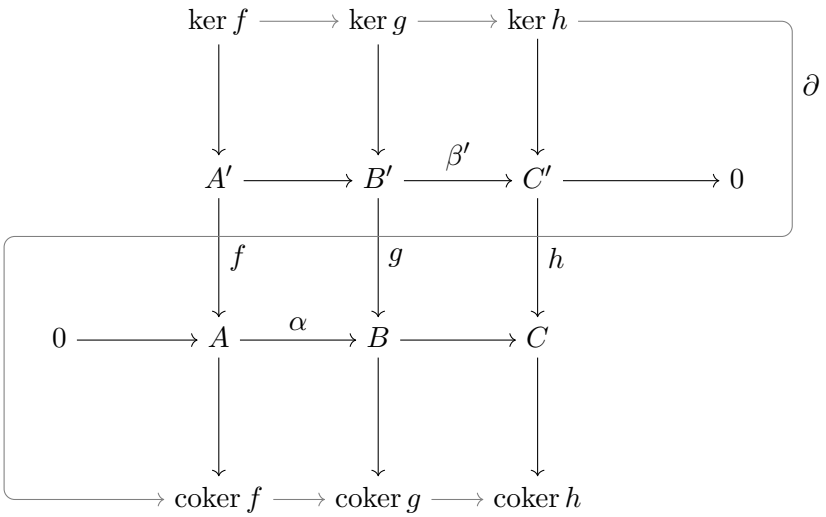
Suppose R is a ring. Consider the following commutative diagram consisting of two (horizontal) exact sequences of R-modules linked by (vertical) R-module homomorphisms.

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & & \end{array}$$

The first goal today is to construct a homomorphism $\partial\colon \ker(h) \to \operatorname{coker}(f)$, called a *connecting homomorphism* so that the sequence

$$\ker(f) \longrightarrow \ker(g) \longrightarrow \ker(h) \xrightarrow{\partial} \operatorname{coker}(f) \longrightarrow \operatorname{coker}(g) \longrightarrow \operatorname{coker}(h)$$

is exact. Thanks to Homeworks 156 and 145 we know that this sequence is exact at both $\ker(g)$ and $\operatorname{coker}(g)$. Thus, we concentrate on constructing[1] ∂. You will verify exactness at $\ker(h)$ and $\operatorname{coker}(f)$ in Homeworks 202 and 223. The following diagram illustrates why this result is often called the *snake lemma*.



(317) Choose $c' \in \ker(h)$.
  (a) Show there is a $b' \in B'$ for which $\beta'(b') = c'$.
  (b) Show that $g(b') \in \alpha(A)$.
  (c) Show there exists a unique $a \in A$ for which $\alpha(a) = g(b')$.
  (d) Show that if $\tilde{b}' \in B'$ with $\beta(\tilde{b}') = c'$, then there exists $a' \in A'$ such that $\alpha(f(a')) = g(b') - g(\tilde{b}')$.
  (e) Conclude that the assignment $c' \mapsto a + \operatorname{im}(f)$ is a well-defined map $\partial\colon \ker(h) \to \operatorname{coker}(f)$.

(318) Is $\partial\colon \ker(h) \to \operatorname{coker}(f)$ an R-module homomorphism?

Here are some quick applications of the snake lemma.

(319) Suppose that R is a ring and M is a finitely presented R-module. Recall that this means there exist finitely generated free R-modules E and F so that

$$E \to F \to M \to 0$$

is exact. Suppose

$$0 \to K \to L \to M \to 0$$

[1] If you need extra help with the construction of ∂, please see the opening scene of the 1980 movie *It's My Turn*.

is exact with L a finitely generated free module. Show that K is finitely generated.

(320) (*Bonus*.) Show that the converse of Prompt 145b is true. Recall that we are looking at the surjective map $R^\ell/AR^t \to R^\ell/K$ induced by the identity map from R^ℓ to R^ℓ.

(321) Suppose R is a ring. Consider the following commutative diagram consisting of two (horizontal) exact sequences of R-modules linked by (vertical) R-module homomorphisms.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

Suppose that two of the three functions in the set $\{f, g, h\}$ are isomorphisms, what, if anything, can you conclude about the third?

Something to Think About

Here is some dialog between Tunococ and Jack Schmidt under the heading *Intuition behind the snake lemma* on Stack Exchange.[1]

> I've been struggling with this for some time. I can prove the Snake Lemma, but I don't really "understand" it. By that I mean if no one told me Snake Lemma existed, I would not even attempt to prove it. I believe I am missing some important intuition that tells me that the lemma "could" be true before actually trying to prove it. Please give me some pointers.
>
> A special case is easy to see: Imagine $A \leq A' \leq B = B'$, and $C = B/A$ and $C' = B'/A'$ with the obvious maps from a module M to M'. The kernels are 0, 0, and A'/A. The cokernels are A'/A, 0, 0. The last kernel and the first cokernel are linked.
> The snake lemma is then just one of the isomorphism theorems. As you deform B and B' more, how do the kernels and cokernels deform? The last kernel and first cokernel no longer need be isomorphic, but the kernel and cokernel of that linking (snakey) map can be described in terms of the kernels and cokernels already there. A specific relation is the snake lemma.
> **Example deformation**
> An example deformation might be helpful: distort the $A' \to B' \to C'$ sequence by quotienting out by some $M \leq B$ (imagine $M = IB$ for some ideal I, so we are tensoring the second line with R/I). How does this change the kernels and cokernels?
> The first line is
>
> $$0 \to A \to B \to B/A \to 0,$$
>
> and the second line becomes
>
> $$0 \to (A' + M)/M \to B'/M \to B'/(A' + M) \to 0$$
>
> so the kernels are $A \cap M$, M, and $(A' + M)/A$ and the cokernels become $(A' + M)/(A + M)$, 0, and 0. The last kernel and the first cokernel are related, but not equal. One clearly has the relation $0 \to (A + M)/A \to (A' + M)/A \to (A' + M)/(A + M) \to 0$ where the last two nonzero terms are the last kernel and the first cokernel. The first term is weird though. We apply another isomorphism theorem to write $(A + M)/A \cong M/(A \cap M)$ and then the solution is clear: We already have $0 \to A \cap M \to M \to M/(M \cap A) \to 0$ so we splice these two together to get the snake lemma:
>
> $$0 \to A \cap M \to M \to (A' + M)/A \to (A' + M)/(A + M) \to 0 \to 0 \to 0$$

Did that help?

[1] https://math.stackexchange.com/questions/182562/intuition-behind-snake-lemma

Please report any errors you find to smdbackr@umich.edu

Worksheet for 19 Nov 2018
Homological algebra: introduction

Vocabulary: chain complex, homology, resolution, finite, free resolution

Definition. Suppose R is a ring. A *chain complex of R-modules* is a sequence of R-modules and R-module homomorphisms

$$\cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

such that $d_i \circ d_{i+1} = 0$ for all i. The chain complex is often denoted $M_\bullet$ or $(M_\bullet, d_\bullet)$.

We have encountered many chain complexes. For example, every short exact sequence is a chain complex.

Definition. Suppose $M_\bullet$ is a chain complex of R-modules. The *i^{th} homology of $M_\bullet$* is the R-module $\mathrm{H}_i(M_\bullet) := \ker(d_i)/\operatorname{im}(d_{i+1})$.

(322) If $N_\bullet$ is a chain complex of R-modules, then $N_\bullet$ is exact if and only if all of its homology modules are zero.

Eventually, we will define a category whose objects are chain complexes of R-modules. For now we look at a family of complexes that arise fairly often.

(323) Suppose R is a ring and M is an R-module. The main idea explored in this prompt appeared when when we discussed what it meant for a module to be presented.

(a) Show that there is a free R-module F_0 and a map $\varphi \in \mathrm{Hom}_R(F_0, M)$ so that

$$0 \longrightarrow \ker(\varphi) \xrightarrow{\iota} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

is exact. Pop quiz: (T/F) If R is a PID, then $\ker(\varphi)$ is free.

(b) Show that there is a free R-module F_1 and a map $\rho \in \mathrm{Hom}_R(F_1, \ker(\varphi))$ so that

$$0 \longrightarrow \ker(\rho) \longrightarrow F_1 \xrightarrow{\rho} \ker(\varphi) \longrightarrow 0$$

is exact.

(c) Show that

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

is a complex of R-modules where $d_1 = \iota \circ \rho$. Is the complex exact at F_0 and/or M?

(d) Show that we may iterate this process to produce a chain complex $F_\bullet$ of free R-modules

$$\cdots \xrightarrow{d_{j+2}} F_{j+1} \xrightarrow{d_{j+1}} F_j \xrightarrow{d_j} F_{j-1} \xrightarrow{d_{j-1}} \cdots\cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} 0$$

where

$$\mathrm{H}_i(F_\bullet) \simeq \begin{cases} 0 & i \neq 0 \\ M & i = 0 \end{cases}$$

Definition. Suppose R is a ring and N is an R-module. A *(left) resolution* of N is an exact sequence

$$\cdots \longrightarrow Q_n \longrightarrow Q_{n-1} \longrightarrow \cdots\cdots \longrightarrow Q_1 \longrightarrow Q_0 \longrightarrow N \longrightarrow 0$$

where each Q_m is an R-module. A resolution is said to be *finite* provided that only finitely many of the modules Q_m are nonzero.

There are also right resolutions (where arrows originate at the zero module rather than terminate there), but the distinction between left and right is usually clear from context so that we just call both species *resolutions*.

We often abuse language and say that the chain complex $Q_\bullet$ given by

$$\cdots \longrightarrow Q_n \longrightarrow Q_{n-1} \longrightarrow \cdots\cdots \longrightarrow Q_1 \longrightarrow Q_0 \longrightarrow 0$$

is a resolution of N. The only change is at the tail: the sequence $Q_0 \longrightarrow N \longrightarrow 0$ has been changed to $Q_0 \longrightarrow 0$. Note that this is still a complex, sometimes called a *deleted complex*, it just is no longer exact. If fact, we have[1]

$$\mathrm{H}_i(Q_\bullet) \simeq \begin{cases} 0 & i \neq 0 \\ N & i = 0. \end{cases}$$

Various adjectives can be added to the word resolution. E.g., a *free resolution* $Q_\bullet$ is a resolution for which each Q_m is free.

(324) Suppose R is a ring. Show that every R-module has a free resolution.

(325) Suppose R is a PID and M is an R-module. Show that there is a free resolution of M of length at most one. Can there be a free resolution of M of length two? length three? infinite length? [Hint: See Homework 121.]

For the remainder of this worksheet, we will assume that R is a commutative ring. Let M and N be R-modules. Suppose that $F_\bullet$ is a free resolution of M.

(326) Show that the sequence $F_\bullet \otimes_R N$

$$\cdots \xrightarrow{d_{i+2}\otimes_R \mathrm{Id}_N} F_{i+1} \otimes_R N \xrightarrow{d_{i+1}\otimes_R \mathrm{Id}_N} F_i \otimes_R N \xrightarrow{d_i \otimes_R \mathrm{Id}_N} F_{i-1} \otimes_R N \xrightarrow{d_{i-1}\otimes_R \mathrm{Id}_N} \cdots$$

is a chain complex of R-modules.

(327) What is the zeroth homology of the complex in Prompt 326? [When people ask questions like this, they are assuming that the tail of the complex under consideration is

$$\cdots \xrightarrow{d_2\otimes_R \mathrm{Id}_N} F_1 \otimes_R N \xrightarrow{d_1\otimes_R \mathrm{Id}_N} F_0 \otimes_R N \xrightarrow{d_0\otimes_R \mathrm{Id}_N} 0.]$$

(328) Let's look at $\mathbb{Z}/n\mathbb{Z}$ for $n > 1$.

(a) Show that

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu_n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

is a free resolution of $\mathbb{Z}/n\mathbb{Z}$ where $\mu_n(j) = nj$.

(b) Compute the homology modules for the complex that arise from tensoring with $\mathbb{Z}/m\mathbb{Z}$ for $m > 1$. That is, compute the homology modules for the complex

$$0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\mu_n \otimes_{\mathbb{Z}} \mathrm{Id}_{\mathbb{Z}/m\mathbb{Z}}} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

(c) Compute the homology modules for the complex that arises from tensoring with $\mathbb{Q}/\mathbb{Z}$.

(d) Compute the homology modules for the complex that arises from tensoring with $\mathbb{Q}$.

(329) For each $\mathbb{Z}$-module $A \in \{\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}, \mathbb{Q}\}$ that you considered in Prompt 328 there is a connection between the homology modules you calculated and the torsion subgroup ${}_nA = \{a \in A \,|\, na = 0\}$ of A. What is it?

Something to Think About

If you have never dealt with cohomology or homology before, then this worksheet probably feels very artificial.[2] You may be asking questions like: Why introduce an auxiliary sequence of modules? Can we assume that all free resolutions are finite? Why do our resolutions have decreasing indices?

The latter question is a matter of convention and, like choosing a basis, is really a matter of using what is convenient for the problem at hand. When one uses increasing indices, one has cohomology rather than homology, and it all works more or less the same.

The first question is easier to answer if you've seen enough mathematics – homology and cohomology are useful tools for making many otherwise seemingly intractable problems approachable. For example, in this class we have asked (but not answered): when is $IJ = I \cap J$ for ideals I and J in a commutative ring R? (Co)homology will provide an answer.

A bigger issue to think about is this: Suppose R is a ring and M is an R-module. As we have seen, there is not a unique free resolution $Q_\bullet$ of M. How will the homology modules $\mathrm{H}_i(Q_\bullet \otimes_R N)$ reflect this lack of uniqueness?

---

[1] Some people define a resolution of N by saying that it is a chain complex whose homology is concentrated in degree zero and isomorphic to N; this leaves a bit of ambiguity that we later do not want – see [A09, pp. 592–].

[2] "Homology/cohomology is just like anything else in mathematics. At first it may seem strange, but once you understand it, it becomes familiar."
–J.S. Milne

Please report any errors you find to smdbackr@umich.edu

Worksheet for 21 Nov 2018
Homological algebra: the long exact sequence.

Vocabulary: homomorphism of complexes, short exact sequence of complexes, homotopic

Let R be a ring.

Definition. Suppose $M_\bullet$ and $N_\bullet$ are chain complexes of R-modules. A *homomorphism of complexes* $\alpha\colon M_\bullet \to N_\bullet$ is a list of homomorphisms ($\alpha_j \in \mathrm{Hom}_R(M_j, N_j)$) for which the following diagram commutes.

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{d^M_{j+2}} & M_{j+1} & \xrightarrow{d^M_{j+1}} & M_j & \xrightarrow{d^M_j} & M_{j-1} & \xrightarrow{d^M_{j-1}} & \cdots \\
 & & \downarrow{\scriptstyle \alpha_{j+1}} & & \downarrow{\scriptstyle \alpha_j} & & \downarrow{\scriptstyle \alpha_{j-1}} & & \\
\cdots & \xrightarrow{d^N_{j+2}} & N_{j+1} & \xrightarrow{d^N_{j+1}} & N_j & \xrightarrow{d^N_j} & N_{j-1} & \xrightarrow{d^N_{j-1}} & \cdots
\end{array}$$

(330) Suppose $M_\bullet$ and $N_\bullet$ are chain complexes of R-modules, and $\alpha\colon M_\bullet \to N_\bullet$ is a chain complex homomorphism. Show that α naturally induces an R-module homomorphism $\mathrm{H}_j(\alpha) \in \mathrm{Hom}_R(\mathrm{H}_j(M_\bullet), \mathrm{H}_j(N_\bullet))$. The diagram below may be useful.

$$\begin{array}{ccccc}
M_{j+1} & \xrightarrow{d^M_{j+1}} & M_j & \xrightarrow{d^M_j} & M_{j-1} \\
\downarrow{\scriptstyle \alpha_{j+1}} & & \downarrow{\scriptstyle \alpha_j} & & \downarrow{\scriptstyle \alpha_{j-1}} \\
N_{j+1} & \xrightarrow{d^N_{j+1}} & N_j & \xrightarrow{d^N_j} & N_{j-1}
\end{array}$$

Recall that $H_j(M_\bullet) = \ker(d^M_j)/\operatorname{im}(d^M_{j+1})$ and $H_j(N_\bullet) = \ker(d^N_j)/\operatorname{im}(d^N_{j+1})$.

One of the more amazing and useful facts of life is that a short exact sequence of chain complexes produces a long exact sequence in homology.[1]

Definition. Suppose $L_\bullet$, $M_\bullet$, and $N_\bullet$ are chain complexes of R-modules. A *short exact sequence of complexes*

$$0 \longrightarrow L_\bullet \xrightarrow{\alpha} M_\bullet \xrightarrow{\beta} N_\bullet \longrightarrow 0$$

is a sequence of homomorphisms of chain complexes such that

$$0 \longrightarrow L_j \xrightarrow{\alpha_j} M_j \xrightarrow{\beta_j} N_j \longrightarrow 0$$

is a short exact sequence of R-modules for every j.

(331) (long exact sequence in homology) Suppose $0 \longrightarrow L_\bullet \xrightarrow{\alpha} M_\bullet \xrightarrow{\beta} N_\bullet \longrightarrow 0$ is a short-exact sequence of chain complexes. We are going to produce a long exact sequence in homology:

$$\begin{array}{ccccc}
 & & \cdots & & \\
 & \overset{\delta_{j+1}}{\curvearrowright} & & & \\
\mathrm{H}_{j+1}(L_\bullet) & \longrightarrow & \mathrm{H}_{j+1}(M_\bullet) & \longrightarrow & \mathrm{H}_{j+1}(N_\bullet) \\
 & \overset{\delta_j}{\curvearrowright} & & & \\
\mathrm{H}_j(L_\bullet) & \longrightarrow & \mathrm{H}_j(M_\bullet) & \longrightarrow & \mathrm{H}_j(N_\bullet) \\
 & \overset{\delta_{j-1}}{\curvearrowright} & & & \\
\mathrm{H}_{j-1}(L_\bullet) & \longrightarrow & \mathrm{H}_{j-1}(M_\bullet) & \longrightarrow & \mathrm{H}_{j-1}(N_\bullet) \\
 & \overset{\delta_{j-2}}{\curvearrowright} & & & \\
 & & \cdots & &
\end{array}$$

There are many things to verify, and common wisdom says that such verifications are best done on one's own. I'm not so sure that common wisdom is correct on this one; so we will check a few things. A portion of a very large

[1] There are all kinds of (co)homologies in life. A short exact usually produces some sort of long sequence, but it may not be exact. So, be careful.

commutative diagram has been created to help us. (Notice that arrows that were once horizontal are now vertical and *vice-versa*. This is done on purpose.)

$$\begin{array}{ccccccccc}
 & & \downarrow{\scriptstyle d^L_{j+3}} & & \downarrow{\scriptstyle d^M_{j+3}} & & \downarrow{\scriptstyle d^N_{j+3}} & & \\
0 & \longrightarrow & L_{j+2} & \xrightarrow{\alpha_{j+2}} & M_{j+2} & \xrightarrow{\beta_{j+2}} & N_{j+2} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^L_{j+2}} & & \downarrow{\scriptstyle d^M_{j+2}} & & \downarrow{\scriptstyle d^N_{j+2}} & & \\
0 & \longrightarrow & L_{j+1} & \xrightarrow{\alpha_{j+1}} & M_{j+1} & \xrightarrow{\beta_{j+1}} & N_{j+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^L_{j+1}} & & \downarrow{\scriptstyle d^M_{j+1}} & & \downarrow{\scriptstyle d^N_{j+1}} & & \\
0 & \longrightarrow & L_j & \xrightarrow{\alpha_j} & M_j & \xrightarrow{\beta_j} & N_j & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^L_j} & & \downarrow{\scriptstyle d^M_j} & & \downarrow{\scriptstyle d^N_j} & & \\
0 & \longrightarrow & L_{j-1} & \xrightarrow{\alpha_{j-1}} & M_{j-1} & \xrightarrow{\beta_{j-1}} & N_{j-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^L_{j-1}} & & \downarrow{\scriptstyle d^M_{j-1}} & & \downarrow{\scriptstyle d^N_{j-1}} & &
\end{array}$$

(a) Are the rows of the above diagram exact? Are the columns exact?

(b) (i) Show that there is a map $\delta\colon \ker d^N_{j+1} \to L_j/\operatorname{im}(d^L_{j+1})$. [Be sure to check that the map you produce is well-defined.]

(ii) Suppose $n \in \ker(d^N_{j+1})$. Show that $d^M_j(\alpha_j(\delta(n))) = 0$. Conclude that $\delta(n) \in \ker d^L_j$. Hence, we may regard δ as a map from $\ker d^N_{j+1}$ to $\mathrm{H}_j(L_\bullet)$.

(iii) Why does $\ker d^N_{j+1}$ contain $\operatorname{im}(d^N_{j+2})$? If $n \in \operatorname{im}(d^N_{j+2})$, show there is an $m' \in M_{j+2}$ so that $\beta_{j+1}(d^M_{j+2}(m')) = n$. Conclude that $\delta(n)$ is zero.

(iv) Conclude that there is a map $\delta_j\colon \mathrm{H}_{j+1}(N_\bullet) \to \mathrm{H}_j(L_\bullet)$. Is it an R-module map?

(c) Thanks to Prompt 330, we now have a long sequence of R-modules:

$$\cdots \longrightarrow \mathrm{H}_{j+2}(N_\bullet) \xrightarrow{\delta_{j+1}} \mathrm{H}_{j+1}(L_\bullet) \longrightarrow \mathrm{H}_{j+1}(M_\bullet) \longrightarrow \mathrm{H}_{j+1}(N_\bullet) \xrightarrow{\delta_j} \mathrm{H}_j(L_\bullet) \longrightarrow \mathrm{H}_j(M_\bullet) \longrightarrow \cdots$$

Show it is exact. [Hint: Leave the bulk of the work for home.]

(332) Suppose $(A_\bullet, d^A_\bullet)$ and $(B_\bullet, d^B_\bullet)$ are two complexes and $f, g\colon A_\bullet \to B_\bullet$ are two chain complex homomorphisms. From Prompt 330 we know that f and g induce maps $\mathrm{H}(f), \mathrm{H}(g)\colon \mathrm{H}(A_\bullet) \to \mathrm{H}(B_\bullet)$. It is natural to ask: when might it be the case that $\mathrm{H}_n(f) = \mathrm{H}_n(g)$? Here we develop one (sufficient, but not necessary) criterion that is useful in practice.

(a) The chain complex homomorphisms f and g are said to be *homotopic* provided that for all $n \in \mathbb{Z}$ there exists $h_n \in \operatorname{Hom}_R(A_n, B_{n+1})$ such that

$$f_n - g_n = d^B_{n+1}h_n + h_{n-1}d^A_n.$$

Use the diagram below to trace through what this definition means.

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{d^A_{n+2}} & A_{n+1} & \xrightarrow{d^A_{n+1}} & A_n & \xrightarrow{d^A_n} & A_{n-1} & \xrightarrow{d^A_{n-1}} & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \xrightarrow{d^B_{n+2}} & B_{n+1} & \xrightarrow{d^B_{n+1}} & B_n & \xrightarrow{d^B_n} & B_{n-1} & \xrightarrow{d^B_{n-1}} & \cdots
\end{array}$$

(b) We wish to show that $\mathrm{H}(f_\bullet) = \mathrm{H}(g_\bullet)$. Suppose $\bar{a} \in \mathrm{H}_n(A) = \ker(d^A_n)/\operatorname{im}(d^A_{n+1})$. Why is it enough to show that if $a \in \ker(d^A_n)$ represents $\bar{a}$, then $f_n(a) - g_n(a) \in \operatorname{im}(d^B_{n+1})$?

(c) Show that if $f_\bullet$ and $g_\bullet$ are homotopic, then $\mathrm{H}(f_\bullet) = \mathrm{H}(g_\bullet)$.

(d) Is homotopy an equivalence relation on chain complex homomorphisms?

Something to Think About

Suppose R is a commutative ring and M is an R-module. Tensoring with M is a right exact functor. Homology will help us understand/measure the failure of the left exactness of this functor. How would you proceed?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 26 Nov 2018
Homological algebra: derived functors

Vocabulary: injective, additive functor, nth right-derived functor, nth left-derived functor

Suppose R is a ring and X is an R-module. In Prompt 323 we showed that X admits a (deleted[1]) projective[2] resolution

$$\cdots \longrightarrow Q_n \longrightarrow Q_{n-1} \longrightarrow \cdots\cdots \longrightarrow Q_1 \longrightarrow Q_0 \longrightarrow 0.$$

Do (deleted) injective resolutions exist? Recall:

Definition. An R-module I is said to be *injective* provided that for every exact sequence $0 \longrightarrow L \longrightarrow M$ of R-modules and for every $g \in \mathrm{Hom}_R(L, I)$ there exists $\tilde{g} \in \mathrm{Hom}_R(M, I)$ so that the following diagram commutes

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & M \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \tilde{g}} & \\ & & I & & \end{array}$$

Thanks to Homework 207 we know[3] that for each R-module Y there is an injective R-module I with $Y \subset I$.

(333) Suppose M is an R-module.

(a) Show that M admits a (right) injective resolution[4]

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots\cdots \longrightarrow I^{n-1} \longrightarrow I^n \longrightarrow \cdots$$

[Hint: Imitate Prompt 323, but reverse the arrows and look at cokernels rather than kernels.]

(b) What is the cohomology of the deleted resolution $0 \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots$

Suppose M is an R-module and $P_\bullet$, $P'_\bullet$ are two projective resolutions of M. Prompt 334 establishes that any two chain complex homomorphisms from $P_\bullet$ to $P'_\bullet$ are homotopic, and Prompt 335 establishes a similar result for injective resolutions of M.

(334) Suppose M and N are R modules. Let $(P_\bullet, d_\bullet)$ and $(P'_\bullet, d'_\bullet)$ be (left) projective resolutions of M and N.

(a) Suppose $\varphi \in \mathrm{Hom}_R(M, N)$. Show that there is a homomorphism of complexes $f\colon P_\bullet \to P'_\bullet$ with $f_{-1} = \varphi$. That is, show that for all $n \in \mathbb{Z}_{\geq 0}$ there exists $f_n \in \mathrm{Hom}_R(P_n, P'_n)$ such that the following diagram

$$\begin{array}{ccccccccccc} \cdots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \varphi} & & \\ \cdots & \xrightarrow{d'_3} & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{d'_0} & N & \longrightarrow & 0 \end{array}$$

commutes. [Hint: for the inductive step look at $\mathrm{im}(f_n \circ d_{n+1}) \subset \ker d'_n$.]

(b) Suppose there is a second homomorphism of complexes $f'\colon P_\bullet \to P'_\bullet$ with $f'_{-1} = \varphi$. Show that f and f' are homotopic. [Hint: Recall that you want to construct maps $h_n \in \mathrm{Hom}_R(P_n, P'_{n+1})$ for which $f_n - f'_n = d'_{n+1}h_n + h_{n-1}d_n$. Show $f_n - f'_n - h_{n-1}d_n\colon P_n \to P'_n$ has image in $\ker(d'_n)$. Define h_n to be the map that extends, via projectivity, $f_n - f'_n - h_{n-1}d_n\colon P_n \to P'_n/\ker(d'_n) \to 0$.]

(335) Suppose M and N are R modules. Let $(I^\bullet, d_I^\bullet)$ and $(J^\bullet, d_J^\bullet)$ be (right) injective resolutions of M and N.

(a) Suppose $\varphi \in \mathrm{Hom}_R(M, N)$. Show that there is a homomorphism of complexes $g\colon I^\bullet \to J^\bullet$ with $g^{-1} = \varphi$. That is, show that for all $n \in \mathbb{Z}_{\geq 0}$ there exists $g^n \in \mathrm{Hom}_R(I^n, J^n)$ such that the following diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \xrightarrow{d_I^{-1}} & I^0 & \xrightarrow{d_I^0} & I^1 & \xrightarrow{d_I^1} & I^2 & \xrightarrow{d_I^2} & \cdots \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle g^0} & & \downarrow{\scriptstyle g^1} & & \downarrow{\scriptstyle g^2} & & \\ 0 & \longrightarrow & N & \xrightarrow{d_J^{-1}} & J^0 & \xrightarrow{d_J^0} & J^1 & \xrightarrow{d_J^1} & J^2 & \xrightarrow{d_J^2} & \cdots \end{array}$$

[1] that is, $\mathrm{H}_i(Q_\bullet) = 0$ if $i \neq 0$ and $\mathrm{H}_0(Q_\bullet) \simeq X$.

[2] Actually, we showed that M admits a free resolution, but every free R-module is projective thanks to Homework 172.

[3] We only considered commutative rings, for non-commutative rings, see [Lan02, XX §4]

[4] Really a coresolution – but nobody uses this terminology.

commutes. [Hint: For the inductive step look at the cokernels $I^n/\operatorname{im}(d_I^{n-1})$.]

(b) Suppose ℓ is a second homomorphism of complexes $\ell\colon I^\bullet \to J^\bullet$ with $\ell^{-1} = \varphi$. Show that g and ℓ are homotopic. [Hint: Recall that you want to construct maps $h^n \in \operatorname{Hom}_R(I^n, J^{n-1})$ so that $g^n - \ell^n = d_J^{n-1}h^n + h^{n+1}d_I^n$. Show $g^n - \ell^n - d_J^{n-1}h^n\colon I^n \to J^n$ vanishes on $\operatorname{im}(d_I^{n-1})$ and then define h^{n+1} to be the map that extends, via injectivity, $f_n - g_n - d_J^{n-1}h^n\colon I^n/\operatorname{im}(d_I^{n-1}) \to J^n$.]

We are now going to apply functors to our (co)resolutions and take (co)homology. Which type of resolution: projective or injective? For covariant functors, one has:

- right exact $\leftrightarrow$ (left) projective resolution $\leftrightarrow$ homology
- left exact $\leftrightarrow$ (right) injective resolution $\leftrightarrow$ cohomology

(336) Make a similar chart for contravariant functors. What's the "rule"?

For our purposes general functors are, well, a bit too general. We are going to restrict our attention to additive functors from the category of R-modules to the category of $\mathbb{Z}$-modules. (Reality check: what's the category of $\mathbb{Z}$-modules?)

Definition. An *additive functor* or *covariant additive functor* from the category of R-modules to the category of $\mathbb{Z}$-modules is a mapping that assigns to every R-module M an abelian group $F(M)$ and assigns to every morphism $f \in \operatorname{Hom}_R(M,N)$ between R-modules M and N a morphism $F(f) \in \operatorname{Hom}_{\mathbb{Z}}(F(M),F(N))$ such that the following properties hold:

- $F(\operatorname{Id}_M) = \operatorname{Id}_{F(M)}$ for all R-modules M.
- $F(g\circ f) = F(g)\circ F(f)$ for all $f \in \operatorname{Hom}_R(M,N)$ and $g \in \operatorname{Hom}_R(N,P)$ and all R-modules M, N, P, and
- $F(f_1+f_2) = F(f_1)+F(f_2)$ for all $f_i \in \operatorname{Hom}_R(M,M')$ and all R-modules M, M'.

The notion of *contravariant additive functor* is defined in a similar fashion.

(337) Suppose M is an R-module.

(a) Show that $Y \mapsto \operatorname{Hom}_{\mathbb{Z}}(Y,M)$ is a left-exact contravariant additive functor from the category of R-modules to the category of $\mathbb{Z}$-modules. (Why $\mathbb{Z}$-modules and not R-modules?)

(b) Show that if R is commutative, then $X \mapsto X \otimes_R M$ is a right-exact additive functor from the category of R-modules to the category of $\mathbb{Z}$-modules. (Why $\mathbb{Z}$-modules and not R-modules?)

(338) Suppose F is a right exact additive functor from the category of R-modules to the category of $\mathbb{Z}$-modules. Suppose M is an R-module and let $(P_\bullet, d_\bullet)$ be a (left) projective resolution of M.

(a) Show that $\cdots \longrightarrow F(P_n) \xrightarrow{F(d_n)} F(P_{n-1}) \xrightarrow{F(d_{n-1})} \cdots\cdots \xrightarrow{F(d_2)} F(P_1) \xrightarrow{F(d_1)} F(P_0) \longrightarrow 0$ is a complex of $\mathbb{Z}$-modules.

(b) Use Prompt 334 and Prompt 332 to conclude that $L_nF(M) := \operatorname{H}_n(F(P_\bullet))$ is well-defined (up to unique isomorphism) and independent of the choice of projective resolution. We call $M \mapsto L^nF(M)$ the *nth left-derived functor of* F. [Hint: Take $\varphi = \operatorname{Id}_M$ and use the additivity of F.]

(c) What is $L_0F(M)$?

(339) Suppose F is a left exact additive functor from the category of R-modules to the category of $\mathbb{Z}$-modules. Suppose M is an R-module and let $(I^\bullet, d^\bullet)$ be a (right) injective resolution of M.

(a) Show that $0 \longrightarrow F(I^0) \xrightarrow{F(d_I^0)} F(I^1) \xrightarrow{F(d_I^1)} \cdots\cdots \xrightarrow{F(d_I^{n-2})} F(I^{n-1}) \xrightarrow{F(d_I^{n-1})} F(I^n) \xrightarrow{F(d_I^n)} \cdots$ is a complex of $\mathbb{Z}$-modules.

(b) Use Prompt 335 and Prompt 332 to conclude that $R^nF(M) := \operatorname{H}^n(F(I^\bullet))$ is well-defined (up to unique isomorphism) and independent of the choice of injective resolution. We call $M \mapsto R^nF(M)$ the *nth right-derived functor of* F. [Hint: Take $\varphi = \operatorname{Id}_M$ and use the additivity of F.]

(c) What is $R^0F(M)$?

Something to Think About

We call R^nF a functor. Is it? Given an R-module M, we certainly get a $\mathbb{Z}$-module $R^nF(M)$. However, if N is another R-module and $\alpha \in \operatorname{Hom}_R(M,N)$, is there a corresponding morphism $R^nF(\alpha) \in \operatorname{Hom}_{\mathbb{Z}}(F(M),F(N))$? What about L^nF; is it a functor?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 28 Nov 2018
Homological algebra: Ext **and** Tor

Vocabulary: Ext, Tor

Suppose R is a ring.

(340) Suppose F is an additive right exact functor from the category of R-modules to the category of $\mathbb{Z}$-modules.
  (a) Recall the construction of the nth left-derived functor of F.
  (b) Show that the nth left-derived functor of F is a functor from the category of R-modules to the category of $\mathbb{Z}$-modules.

(341) Suppose F is an additive left exact functor from the category of R-modules to the category of $\mathbb{Z}$-modules.
  (a) Recall the construction of the nth right-derived functor of F.
  (b) Show that the nth right-derived functor of F is a functor from the category of R-modules to the category of $\mathbb{Z}$-modules.

The derived functors associated to "tensoring" and "taking homomorphisms" provide a rich source of examples for the homological machinery we have developed/will develop.

Definition. Suppose R is a commutative ring and M is an R-module. The nth left-derived functor of tensoring by M (i.e., the right-exact functor $Y \mapsto M \otimes_R Y$) is denoted by $\operatorname{Tor}_n(M, \cdot)$ or $\operatorname{Tor}_n^R(M, \cdot)$.

(342) Suppose that S is a commutative ring and N, M are S-modules. Compute $\operatorname{Tor}_0^S(M, N)$.

(343) Suppose $m, n \in \mathbb{Z}_{>1}$. Compute $\operatorname{Tor}_j^{\mathbb{Z}}(A, \mathbb{Z}/n\mathbb{Z})$ for $A \in \{\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}, \mathbb{Q}\}$ and $j \in \mathbb{Z}$. [Hint: See Prompt 328.]

(344) Consider the $\mathbb{Z}/(18)$-module $\mathbb{Z}/(6)$ and let $\varphi \in \operatorname{Hom}_{\mathbb{Z}/(18)}(\mathbb{Z}/(18), \mathbb{Z}/(6))$ be the natural map $\varphi(k + (18)) = k + (6)$.
  (a) Show that $\cdots \xrightarrow{\mu_3} \mathbb{Z}/(18) \xrightarrow{\mu_6} \mathbb{Z}/(18) \xrightarrow{\mu_3} \mathbb{Z}/(18) \xrightarrow{\mu_6} \mathbb{Z}/(18) \xrightarrow{\varphi} \mathbb{Z}/(6) \longrightarrow 0$ is a projective resolution of $\mathbb{Z}/(6)$. Here $\mu_j(k) = jk$.
  (b) Suppose M is a $\mathbb{Z}/(18)$-module. Show

$$\operatorname{Tor}_n^{\mathbb{Z}/(18)}(M, \mathbb{Z}/(6)) \simeq \begin{cases} M/6M & n = 0 \\ {}_6M/3M & n \in \mathbb{Z}_{\geq 1} \text{ and odd} \\ {}_3M/6M & n \in \mathbb{Z}_{\geq 1} \text{ and even.} \end{cases}$$

  Here ${}_kM = \{m \in M \mid km = 0\}$.

Definition. Suppose R is a ring and M is an R-module. The nth right-derived functor of the (covariant) left exact functor $Z \mapsto \operatorname{Hom}_R(M, Z)$ is denoted by $\operatorname{Ext}^n(M, \cdot)$ or $\operatorname{Ext}_R^n(M, \cdot)$.

Suppose N is an R module. One could just as easily have considered the nth right-derived functor of the *contravariant* left exact functor $Y \mapsto \operatorname{Hom}_R(Y, N)$ and called the resulting *homology* groups $\operatorname{ext}_n(\cdot, N)$. It turns out (see [Jac89, p. 353] or [A09, p. 677]) that $\operatorname{ext}_n(M, N) \simeq \operatorname{Ext}^n(M, N)$ for all R-modules M and N, so which approach you use is a matter of personal preference and convenience. Everyone uses the notation Ext for either.

(345) Suppose that S is a ring and N, M are S-modules. Compute $\operatorname{Ext}_S^0(M, N)$.

(346) We need some injectives so that we can compute. Suppose $m \in \mathbb{Z}_{>1}$ and $I \leq \mathbb{Z}/(m)$ is an ideal.
  (a) Show that there exists $k \in \mathbb{Z}$ with $k \mid m$ such that $I = k\mathbb{Z}/(m)$. Conclude that if $d = \frac{m}{k}$, then $I =_d \mathbb{Z}/(m) = \{x \in \mathbb{Z}/(m) \mid dx = 0\}$.
  (b) Suppose $f \in \operatorname{Hom}_{\mathbb{Z}/(m)}(I, \mathbb{Z}/(m))$. Show that there exists $\ell \in \mathbb{Z}/(m)$ for which $f(i) = \ell i$ for all $i \in I$. Conclude that there exists $\tilde{f} \in \operatorname{Hom}_{\mathbb{Z}/(m)}(\mathbb{Z}/(m), \mathbb{Z}/(m))$ for which $\operatorname{res}_I \tilde{f} = f$.
  (c) Show that $\mathbb{Z}/(m)$ is an injective $\mathbb{Z}/(m)$-module. [Hint: Imitate the proof of Homework 161.]
  (d) (*Bonus.*) More generally, if R is a PID and $a \in R$, show $R/(a)$ is an injective $R/(a)$-module.

(347) Consider the $\mathbb{Z}/(18)$-module $\mathbb{Z}/(6)$ and let $\psi \in \operatorname{Hom}_{\mathbb{Z}/(18)}(\mathbb{Z}/(6), \mathbb{Z}/(18))$ be the natural map $\psi(k + (6)) = 3k + (18)$.
  (a) Show that $0 \longrightarrow \mathbb{Z}/(6) \xrightarrow{\psi} \mathbb{Z}/(18) \xrightarrow{\mu_6} \mathbb{Z}/(18) \xrightarrow{\mu_3} \mathbb{Z}/(18) \xrightarrow{\mu_6} \mathbb{Z}/(18) \xrightarrow{\mu_3} \cdots$ is an injective resolution of $\mathbb{Z}/(6)$. Here $\mu_j(k) = jk$.

(b) Suppose M is a $\mathbb{Z}/(18)$-module. Show

$$\mathrm{Ext}^n_{\mathbb{Z}/(18)}(\mathbb{Z}/(6), M) \simeq \begin{cases} {}_6M & n = 0 \\ {}_3M/6M & n \in \mathbb{Z}_{\geq 1} \text{ and odd} \\ {}_6M/3M & n \in \mathbb{Z}_{\geq 1} \text{ and even.} \end{cases}$$

Here ${}_kM = \{m \in M \mid km = 0\}$. [Caution: Do we use a projective or an injective resolution?]

(c) Suppose M is a $\mathbb{Z}/(18)$-module. Compute $\mathrm{Ext}^n_{\mathbb{Z}/(18)}(M, \mathbb{Z}/(6))$. [Caution: Do we use a projective or an injective resolution? Also, your answer may not be pretty.]

Before continuing on, we need to examine how derived functors interact with exact sequences.

(348) Review Prompt 331.

(349) Suppose that R is a ring and $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence of R-modules. Let $\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow L \longrightarrow 0$ and $\cdots \longrightarrow Q_1 \longrightarrow Q_0 \longrightarrow N \longrightarrow 0$ be projective resolutions of L and N, respectively.

(a) Show that for each n we have $P_n \oplus Q_n$ is a projective R-module.

(b) Show that $\cdots \longrightarrow P_1 \oplus Q_1 \longrightarrow P_0 \oplus Q_0 \longrightarrow M \longrightarrow 0$ is a projective resolution of M such that the following diagram has exact columns, exact rows, and commutes.

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_2 & \longrightarrow & P_2 \oplus Q_2 & \longrightarrow & Q_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_1 & \longrightarrow & P_1 \oplus Q_1 & \longrightarrow & Q_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0 & \longrightarrow & P_0 \oplus Q_0 & \longrightarrow & Q_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

(c) Conclude that if F is an additive right-exact functor from the category of R-modules to the category of $\mathbb{Z}$-modules, then we have a long exact sequence

$$\cdots \longrightarrow L_{j+2}F(N) \xrightarrow{\delta_{j+1}} L_{j+1}F(L) \longrightarrow L_{j+1}F(M) \longrightarrow L_{j+1}F(N) \xrightarrow{\delta_j} L_jF(L) \longrightarrow L_jF(M) \longrightarrow \cdots$$

that ends with

$$\cdots \longrightarrow L_1F(N) \xrightarrow{\delta_0} F(L) \longrightarrow F(M) \longrightarrow F(N) \longrightarrow 0$$

In Homework 215 you will establish the same result for right-derived functors arising from additive left exact functors.

Something to Think About

As you noticed in Prompt 329, the functor Tor has something to do with measuring torsion. In Homework 217 you will cement the relationship by showing that for R a commutative ring and $r \in R$ a non-zero-divisor we have $\mathrm{Tor}^R_1(N, R/(r)) \simeq {}_rN$ for all R-modules N. Here ${}_rN$ is the R-module of r-torsion elements of N, that is, ${}_rN = \{n \in N \mid rn = 0\}$. What might $\mathrm{Ext}^1(M, N)$ measure?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 30 Nov 2018
Homological algebra: flatness & extensions

Vocabulary: flat, extensions of M by N, trivial extension

(350) Suppose R is a ring. Show that the following conditions on an R-module M are equivalent.
- M is injective.
- $\mathrm{Ext}^1_R(N, M) = 0$ for all R-modules N.
- $\mathrm{Ext}^n_R(N, M) = 0$ for all $n > 0$ and all R-modules N.

[Hint: Use Homework 215.]

In Homework 214 you will show that an R-module N is projective R-module iff $\mathrm{Ext}^1_R(N, M) = 0$ for all R-modules M iff $\mathrm{Ext}^n_R(N, M) = 0$ for all n and all R-modules M. Since we know that (a) $Y \mapsto \mathrm{Hom}_R(Y, M)$ is exact if and only if M is injective and (b) $X \mapsto \mathrm{Hom}_R(M, X)$ is exact if and only if M is projective, the equivalencies established in Prompt 350 and Homework 214 are not unexpected.

On the other hand, we have not yet given a name to those modules M for which $Z \mapsto Z \otimes_R M$ is exact.

(351) Suppose R is a commutative ring. Show that the following conditions on an R-module M are equivalent.
- Tensoring by M is exact.
- $\mathrm{Tor}^R_1(M, N) = 0$ for all R-modules N.
- $\mathrm{Tor}^R_n(M, N) = 0$ for all $n > 0$ and all R-modules N.

[Hint: Use Prompt 331.]

Definition. Suppose R is a commutative ring. An R-module M that satisfies any of the equivalent conditions of Prompt 351 is said to be *flat*.

What sorts of modules are flat?

(352) Suppose R is commutative. Show that R is a flat R-module.

(353) Suppose R is a commutative ring and F is a free R-module. Show that F is a flat R-module. What does this say about modules over a field k?

Just as every free module is projective, in Homework 212 you will show that ever projective module is flat. Is every flat module projective? Is every injective module flat? Is every flat module injective?

(354) Show that $\mathbb{Q}$ is a flat but not projective $\mathbb{Z}$-module. [Hint: Use Homework 209.]

(355) Show that $\mathbb{Q}/\mathbb{Z}$ is an injective, but not flat, $\mathbb{Z}$-module. [Hint: $0 \to \mathbb{Z} \to \mathbb{Q}$.]

(356) Is every flat module injective?

Suppose R is a commutative ring and M, N are R-modules. We have shown that $M \otimes_R N \simeq N \otimes_R M$. It turns out that the same is true (see [A09, p. 676]) for Tor^R_n:

$$\mathrm{Tor}^R_n(M, N) \simeq \mathrm{Tor}^R_n(N, M).$$

Suppose R is any ring and M and N are R-modules. We now show that $\mathrm{Ext}^1(M, N)$ measures the extensions[1] of M by N. Let $E(M, N)$ denote the set of extensions of M by N. Given $\tilde{E}_i = \; 0 \longrightarrow N \longrightarrow E_i \longrightarrow M \longrightarrow 0 \; \in E(M, N)$ for $i \in \{1, 2\}$ we say that $\tilde{E}_1$ is equivalent to $\tilde{E}_2$ provided that there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E_1 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_N} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}_M} & & \\ 0 & \longrightarrow & N & \longrightarrow & E_2 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

[What sort of map must the middle vertical arrow be?] When this happens, we write $\tilde{E}_1 \sim \tilde{E}_2$.

(357) Show that $\sim$ is an equivalence relation on $E(M, N)$.

Fix $\tilde{E} = \; 0 \longrightarrow N \xrightarrow{\alpha} E \xrightarrow{\beta} M \longrightarrow 0 \; \in E(M, N)$. Suppose P is a projective R-module and $\pi \in \mathrm{Hom}_R(P, M)$ is surjective.

[1] Recall that P is an extension of M by N provided that $0 \to N \to P \to M \to 0$ is exact.

(358) Why does such a P exist?

Let $K = \ker(\pi)$, and let $\iota \in \mathrm{Hom}_R(K, P)$ denote the natural inclusion. Since P is projective, there exists $u \in \mathrm{Hom}_R(P, E)$ for which $\beta \circ u = \pi$. Note that u is not, in general, unique.

(359) Given the choices above, show that there is a unique $\nu \in \mathrm{Hom}_R(K, N)$ such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{\iota} & P & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \mathrm{Id}_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{\alpha} & E & \xrightarrow{\beta} & M & \longrightarrow & 0 \end{array}$$

commutes.

(360) Show that the following sequence is exact.

$$0 \longrightarrow \mathrm{Hom}_R(M, N) \xrightarrow{\pi^*} \mathrm{Hom}_R(P, N) \xrightarrow{\iota^*} \mathrm{Hom}_R(K, N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow 0$$

(361) Note that $\nu \in \mathrm{Hom}_R(K, N)$, so it defines an element $\bar{\nu}$ of $\mathrm{Ext}^1_R(M, N) \simeq \mathrm{coker}\, \iota^*$.

(a) Show that the image of ν in $\mathrm{Ext}^1_R(M, N)$ does not depend on the choice of u, and so we have a map $E(M, N) \to \mathrm{Ext}^1_R(M, N)$ given by $\tilde{E} \mapsto \bar{\nu} = \bar{\nu}(\tilde{E})$.

(b) Show that if $E = N \oplus M$, then $\bar{\nu} = 0$. This is why $N \oplus M$ is called the *trivial extension* of M by N.

(c) Show that the map $\tilde{E} \mapsto \bar{\nu} = \bar{\nu}(\tilde{E})$ descends to a map from $E(M, N)/\!\sim$ to $\mathrm{Ext}^1_R(M, N)$.

(362) (*Bonus*.) Construct an inverse map. That is, construct a map $e\colon \mathrm{Ext}^1_R(M, N) \to E(M, N)$ such that (a) for $\kappa \in \mathrm{Ext}^1_R(M, N)$ we have $\kappa = \bar{\nu}(e(\kappa))$ and (b) for $\tilde{E} \in E(M, N)$ we have $e(\bar{\nu}(\tilde{E})) \sim \tilde{E}$. [See Homework 219.]

(363) Conclude that $\mathrm{Ext}^1_R(M, N)$ measures the extensions of M by N up to natural equivalence.

(364) Consider the $\mathbb{Z}/(18)$-modules $\mathbb{Z}/(6)$ and $\mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$. Up to equivalence, how many extensions of $\mathbb{Z}/(6)$ by $\mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$ are there?

Something to Think About

Since $\mathrm{Ext}^1_R(M, N)$ measures the number of extensions of M by N, what might $\mathrm{Ext}^2(M, N)$ measure? It turns out that $\mathrm{Ext}^2(M, N)$ and higher Exts measure something very similar.[1] For example, $\mathrm{Ext}^2_R(M, N)$ measures the *two-step extensions*

$$0 \longrightarrow N \longrightarrow E_1 \longrightarrow E_2 \longrightarrow M \longrightarrow 0$$

of M by N up to a natural equivalence. Can you formulate when two two-step extensions might be equivalent? Can you think of a situation where understanding the two-step extensions might be important?

[1] See Yoneda, Nobuo, *On* Ext *and exact sequences*, J. Fac. Sci. Univ. Tokyo Sect. I, **8**, 1960, pp. 507–576.

Please report any errors you find to smdbackr@umich.edu

Worksheet for 3 Dec 2018
Homological algebra: Koszul complexes

Vocabulary: Koszul complex

Suppose R is a commutative ring. Because they are explicit, fairly easy to compute with, and measure important invariants, Koszul[1] complexes are useful in commutative algebra and algebraic geometry. The goal here is to provide a gentle introduction to their definition.

(365) Suppose k is a field.

(a) Consider

$$0 \longrightarrow k[x] \xrightarrow{\mu_x} k[x] \xrightarrow{\pi} k \longrightarrow 0$$

where $\pi\colon k[x] \to k \simeq k[x]/(x)$ is the natural projection. Prove that this is an exact sequence of k-modules.

(b) Consider

$$0 \longrightarrow k[x,y] \xrightarrow{d_2} k[x,y] \oplus k[x,y] \xrightarrow{d_1} k[x,y] \xrightarrow{\pi} k \longrightarrow 0$$

where $\pi\colon k[x,y] \to k \simeq k[x,y]/(x,y)$ is the natural projection, $d_1(f,g) = fx+gy$, and $d_2(h) = (hx, -hy)$. Prove that this is an exact sequence of k-modules.

(c) Consider

$$0 \longrightarrow k[x,y,z] \xrightarrow{d_3} k[x,y,z]^{\oplus 3} \xrightarrow{d_2} k[x,y,z]^{\oplus 3} \xrightarrow{d_1} k[x,y,z] \xrightarrow{\pi} k \longrightarrow 0$$

where $\pi\colon k[x,y,z] \to k \simeq k[x,y,z]/(x,y,z)$ is the natural projection, $d_1(f,g,h) = fx + gy + hz$, $d_2(f',g',h') = (-zg' + yh', -zf' + xh', -yf' + xg')$, and $d_3(f'') = (xf'', yf'', zf'')$. Prove that this is an exact sequence of k-modules.

This is a very explicit way to create a free resolution of k. Was the fact that k is a field important? How to generalize beyond three variables? How to generalize this construction from $k[x]$ to R? [Yes, I mean R, not $R[x]$.] You should give this latter question some thought before proceeding – the answer below is an algebra meme.[2]

(366) Suppose $a \in R$. Consider

$$0 \longrightarrow R \xrightarrow{\mu_a} R \xrightarrow{\pi} R/(a) \longrightarrow 0$$

where π is the canonical projection and $\mu_a(r) = ar$.

(a) Prove that this is a complex.

(b) Prove that if a is a non-zero-divisor in R, then the sequence is exact.

(367) Suppose $a, b \in R$. Consider

$$0 \longrightarrow R \xrightarrow{d_2} R \oplus R \xrightarrow{d_1} R \xrightarrow{\pi} R/(a,b) \longrightarrow 0$$

where π is the canonical projection, $d_1(r,s) = ra + sb$, and $d_2(t) = (bt, -at)$.

(a) Prove that this is a complex.

(b) Prove that if a is a non-zero-divisor in R and b is a non-zero-divsor modulo (a) (i.e., $b+(a)$ is a non-zero-divsor in $R/(a)$), then the sequence is exact.

(368) Suppose $a, b, c \in R$. Consider

$$0 \longrightarrow R \xrightarrow{d_3} R \oplus R \oplus R \xrightarrow{d_2} R \oplus R \oplus R \xrightarrow{d_1} R \xrightarrow{\pi} R/(a,b,c) \longrightarrow 0$$

where π is the canonical projection, $d_1(r,s,t) = ra + sb + tc$, $d_2(u,v,w) = (-cv + bw, -cu + aw, -bu + av)$, and $d_3(z) = (az, -bz, cz)$.

(a) Prove that this is a complex. [I found it useful to write down matrices for the maps.]

(b) Prove that if a is a non-zero-divisor in R, b is a non-zero-divsor modulo (a), and c is a non-zero-divisor module (a,b) (i.e., $b + (a,b)$ is a non-zero-divsor in $R/(a,b)$, then the sequence is exact.

[1] Named for Jean-Louis Koszul (1921-2018).

[2] *meme* noun. an element of a culture or system of behavior that may be considered to be passed from one individual to another by nongenetic means, especially imitation. (defintion provided by google)

How to generalize this to ideals with four or more generators? You should give this some thought before proceeding.

(369) Suppose $a_1, a_2, \ldots, a_n \in R$. Let $I = (a_1, a_2, \ldots, a_n)$. Consider

$$(*) \qquad 0 \longrightarrow R \simeq \bigwedge^n(R^n) \xrightarrow{d_n} \bigwedge^{n-1}(R^n) \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} \bigwedge^0(R^n) = R \xrightarrow{\pi} R/I \longrightarrow 0$$

where π is the natural projection and $d_r \in \mathrm{Hom}_R(\bigwedge^r(R^n), \bigwedge^{r-1}(R^n))$ is defined (on basis elements) by

$$d_r(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_r}) = \sum_{j=1}^{r} (-1)^{j+1} a_{i_j}\, e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_r}$$

where the hatted element is deleted.

(a) Show that Prompts 366, 367, and 368 correspond to $n \in \{1, 2, 3\}$ in (*).
(b) Show that (*) is a complex.
(c) Conjecture conditions on $a_1, a_2, \ldots, a_n$ that will ensure that (*) is exact.
(d) (*Bonus*.) Verify your conjecture.

Definition. Suppose R is a commutative ring and $\varphi \in \mathrm{Hom}_R(R^{\oplus n}, R)$. Define $d_r \in \mathrm{Hom}_R(\bigwedge^r(R^{\oplus n}), \bigwedge^{r-1}(R^{\oplus n}))$ on basis elements by

$$d_r(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_r}) = \sum_{j=1}^{r} (-1)^{j+1} \varphi(e_{i_j})\, e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_r}$$

where the hatted element is deleted. The resulting complex

$$0 \longrightarrow \bigwedge^n(R^{\oplus n}) \xrightarrow{d_n} \bigwedge^{n-1}(R^{\oplus n}) \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} \bigwedge^0(R^{\oplus n}) = R \xrightarrow{\pi} R/\operatorname{im}(\varphi) \longrightarrow 0$$

is the *Koszul complex associated to* φ. The map π is the natural projection.

(370) Show that the complex considered in Prompt 369 is a Koszul complex.

Something to Think About

We could have more easily defined a map $d^r \in \mathrm{Hom}_R(\bigwedge^r(R^{\oplus n}), \bigwedge^{r+1}(R^{\oplus n}))$ by fixing $v \in R^{\oplus n}$ and setting

$$d^r(x) = v \wedge x.$$

for $r > 0$ and $d^0(1) = v$. Can you, in under five seconds, show that

$$0 \longrightarrow \bigwedge^0(R^{\oplus n}) = R \xrightarrow{d^0} \bigwedge^1(R^{\oplus n}) \xrightarrow{d_1} \cdots \xrightarrow{d^{n-1}} \bigwedge^n(R^{\oplus n}) \longrightarrow 0$$

is a complex? Does the resulting complex (also called a Koszul complex) have any desirable properties? [Yes.]

Please report any errors you find to smdbackr@umich.edu

Worksheet for 5 Dec 2018
Group cohomology: introduction

Vocabulary: group algebra of G, convolution, ring of Laurent polynomials, group action, R-action, (G,R)-modules, set of fixed points, automorphism group of N, $\mathrm{H}^i(G,\cdot)$, augmentation map

Suppose G is a group with identity e and R is a commutative ring. We want to use the mathematics we've developed to study the action of G on various spaces. To do this, we need to produce a ring.

Recall (see Prompt 115) that $\mathrm{Fun}'(G,R)$ denotes the free R-module that consists of functions $f\colon G\to R$ for which $f(g)=0$ for all but finitely many $g\in G$.

Definition. The *group algebra of G over R*, denoted $R[G]$, is the R-module $\mathrm{Fun}'(G,R)$ equipped with the product

$$(f*h)(u)=\sum_{g\in G} f(g)h(g^{-1}u).$$

The operation $*$ is called *convolution*.

Warning! For locally compact Hausdorff groups (places where one can integrate), there is a different definition of group algebra. It specializes to the one above when the topology on G is the discrete topology.

(371) Show that $R[G]$ is an algebra. Does this require R to be commutative?

(372) Does convolution on $R[G]$ have an idenitity? What is it?

(373) Show that $R[\mathbb{Z}]\simeq R[x,x^{-1}]$ as algebras. The algebra $R[x,x^{-1}]$ is called the *ring of Laurent polynomials on R*; the natural product operation gives $R[x,x^{-1}]$ an algebra structure.

(374) Suppose $m\in\mathbb{Z}_{>1}$ and $C_m=\langle c\rangle$ is a cyclic group of order m. Show that $R[C_m]\simeq R[x]/(x^m-1)$ as algebras.

(375) For a non-abelian group like S_3 or $\mathrm{GL}_{43}(\mathbb{C})$, there will not be any "polynomial-ish" way to realize $R[G]$. Why?

In the non-abelian case, it is often useful to think of elements of $R[G]$ as sums of the form $\sum a_g[g]$ with $a_g\in R$ zero for all but finitely many $g\in G$.

Recall that if X is a set, then an action of G on X is a map $G\times X\to X$ such that

- $gh\cdot x=g\cdot(h\cdot x)$ for all $h,g\in G$ and $x\in X$.
- $e\cdot x=x$ for all $x\in X$.

Definition. An *R-action* of G on an R-module M is an action of G on M that also satisfies

- $g\cdot rm=r(g\cdot m)$ for all $r\in R$, $g\in G$, and $m\in M$
- $g\cdot(m+m')=g\cdot m+g\cdot m'$ for all $g\in G$ and $m,m'\in M$

An R-module N equipped with an R-action is called a *(G,R)-module*; its *set of fixed-points* is $N^G=\{n\in N\mid g\cdot n=n \text{ for all } g\in G\}$.

Note that every R-module N is a (G,R)-module with respect to the trivial R-action of G on N.

(376) Suppose L is a (G,R)-module. Show that L^G is a (G,R)-submodule of L.

(377) Show that $R[G]$ is naturally a (G,R)-module. When G is finite, what is is $R[G]^G$?

(378) Show that specifying a G-action on an R-module N is equivalent to specifying a group homomorphism $\varphi\colon G\to \mathrm{Aut}_R(N)=\mathrm{Hom}_R(N,N)^\times$. The group $\mathrm{Aut}_R(N)$ is called the *automorphism group of N*.

(379) Show that every (G,R)-module is naturally an $R[G]$-module and *vice-versa*.

When k is a field, the study of $k[G]$-modules is called *representation theory*.

(380) (*Very Important Example*) A great many counterexamples in this area of mathematics derive from the following example. So, learn it and remember it.

(a) Let $G=\mathbb{Z}$. We define actions of G on R and $R\oplus R$ by
- $g\cdot r=r$ for all $r\in R$ and $g\in G$
- $g\cdot[x,y]^T=[x+gy,y]^T$ for $g\in G$ and $[x,y]^T\in R^{\oplus 2}$.

(i) Show that these are G-actions.

(ii) For $g\in G$, write down the matrix by which g acts with respect to the standard bases (e.g., for the trivial action on $R^{\oplus n}$, the matrix representing the action of $g\in G$ is Id_n).

(iii) Compute the set of G fixed-points of R and $R^{\oplus 2}$ with respect to these actions.

(b) Show that the following sequence is an exact sequence of $R[G]$-modules.

$$0 \longrightarrow R \xrightarrow{\alpha} R \oplus R \xrightarrow{\beta} R \longrightarrow 0$$

where $\alpha(r) = [r, 0]^T$ and $\beta([x, y]^T) = y$.

(c) Show that taking fixed-points is not exact – that is, show that

$$0 \longrightarrow R^G \xrightarrow{\alpha} (R \oplus R)^G \xrightarrow{\beta} R^G \longrightarrow 0$$

is not exact.

Group cohomology provides a way to measure the failure of exactness when taking fixed-points. It is a powerful tool in number theory (e.g., Galois cohomology) and algebra (e.g., classification of central simple algebras). Since the set of fixed-points has nothing to do with the R-structure of our modules,

for the remainder of this worksheet our ring is $\mathbb{Z}$.

(381) Show that $M \mapsto M^G$ is a left-exact additive functor from the category of $\mathbb{Z}[G]$-modules to the category of $\mathbb{Z}$-modules.

The nth right-dervied functor of $M \mapsto M^G$ is denoted $\mathrm{H}^n(G, \cdot)$; it is a functor from $\mathbb{Z}[G]$-modules to $\mathbb{Z}$-modules. Since projective modules are easier to find than injectives, we recognize that

(382) $M^G \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ (where $\mathbb{Z}$ is being thought of as a G-module with trivial action)

and so $\mathrm{H}^n(G, \cdot) \simeq \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, \cdot) \simeq \mathrm{ext}_n(\mathbb{Z}, \cdot)$.

(383) Let $G = C_m$, a cyclic group of order $m \in \mathbb{Z}_{>1}$. Suppose M is a $\mathbb{Z}[C_m]$-module. Recall that $\mathbb{Z}[C_m] \simeq \mathbb{Z}[x]/(x^m - 1)$. [This smells like geometric sums . . .]

(a) Show that the complex below is a projective resolution of $\mathbb{Z}$.

$$\cdots \xrightarrow{\mu_N} \mathbb{Z}[C_m] \xrightarrow{\mu_{(1-x)}} \mathbb{Z}[C_m] \xrightarrow{\mu_N} \mathbb{Z}[C_m] \xrightarrow{\mu_{(1-x)}} \mathbb{Z}[C_m] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where $N = 1 + x + \cdots + x^{m-1}$ and $\varepsilon(\sum c_g[g]) = \sum c_g$. [The map ε is called an *augmentation map*, so called because it "augments the algebra $\mathbb{Z}[G]$."]

(b) Apply the functor $M \mapsto \mathrm{Hom}_{\mathbb{Z}[C_m]}(\cdot, M)$ to the appropriate deleted complex to arrive at the complex

$$0 \longrightarrow M \xrightarrow{\mu_{(1-x)}} M \xrightarrow{\mu_N} M \xrightarrow{\mu_{(1-x)}} M \xrightarrow{\mu_N} \cdots$$

Be sure to explain why we can use the "same" maps rather than, for example, $\mu^*_{(1-x)}$.

(c) Show that

$$\mathrm{H}^i(G, M) = \begin{cases} \ker(\mu_N \colon M \to M)/\mu_{(1-x)}M & \text{if } i > 0 \text{ is odd} \\ M^{C_m}/\mu_N(M) & \text{if } i > 0 \text{ is even} \\ M^{C_m} & \text{if } i = 0 \\ 0 & \text{if } i < 0 \end{cases}$$

Something to Think About

If you did it correctly, then your work in Prompt 383 felt awkwardly specialized to the situation. This is a good time for a very important lesson in mathematics/life: sometimes we do what we do because it works.

A second and related lesson is this: it is probably best to think of Ext^i, Tor_i, H^i, etc. as symbols that represent important things that are often complicated. However, with some cleverness and work, we can understand what these symbols represent when we need to. This is not a foreign idea to you. What is π?

Please report any errors you find to smdbackr@umich.edu

Worksheet for 7 Dec 2018
Group cohomology: the bar or standard resolution

Vocabulary: bar resolution, standard resolution, one-cocycle, crossed-homomorphism, one-coboundary, principal crossed homomorphsim

Suppose G is a group with identity e. There is a standard $\mathbb{Z}[G]$ resolution of $\mathbb{Z}$ that is useful when computing group cohomology – the resolution goes by two names: the *bar resolution* or the *standard resolution*. We will provide an introduction, details are left to the interested reader.

We know that given an exact sequence

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

of $\mathbb{Z}[G]$-modules, we have a long exact sequence

$$0 \longrightarrow A^G \xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G \xrightarrow{\partial} \mathrm{H}^1(G,A) \longrightarrow \mathrm{H}^1(G,B) \longrightarrow \cdots$$

(384) Why do we know that such a long exact sequence exists?

(385) Show: The failure of $\beta\colon B^G \to C^G$ to be surjective is measured by $\ker(\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B))$.

(386) Suppose $c \in C^G$.

(a) Show there exists $b \in B$ such that $\beta(b) = c$.

(b) Show that for all $g \in G$ there exists a unique $a_g \in A$ for which $\alpha(a_g) = gb - b$. Thus, we can define a function $f_{c,b}\colon G \to A$ by $f_{c,b}(g) = a_g$.

(c) Show that for all $x, y \in G$ we have $a_{xy} = xa_y + a_x$; thus $f_{c,b}\colon G \to A$ satisfies $f_{c,b}(xy) = xf_{c,b}(y) + f_{c,b}(x)$ for all $x, y \in G$. Such a function is called a *one-cocycle* or *crossed-homomorphism*[1], and the group (under addition) of such functions is denoted $Z^1(G,A)$.

(d) Suppose $a \in A$. Show that the function $\ell_a\colon G \to A$ given by $\ell_a(g) = ga - a$ is also a one-cocycle, called a *one-coboundary* or *principal crossed homomorphsism*. We let $B^1(G,A)$ denote the subgroup of $Z^1(G,A)$ consisting of one-coboundaries.

(e) Note that for all $a \in A$ we have $f_{c,b} + \ell_a = f_{c,b+\alpha(a)}$. Use the fact that $C \simeq B/\operatorname{im}(\alpha)$ to conclude that the equivalence class represented by $f_{c,b}$ in $Z^1(G,A)/B^1(G,A)$ depends only on c. We denote this equivalency class by f_c.

(f) Show that if $c = \beta(b')$ for some $b' \in B^G$, then $f_c \in Z^1(G,A)/B^1(G,A)$ has trivial image in $Z^1(G,B)/B^1(G,B)$.

Motivated by the above, we guess (correctly) that $\mathrm{H}^1(G,A) \simeq Z^1(G,A)/B^1(G,A)$. This suggests that we should look to calculate $\mathrm{H}^n(G,A)$ by choosing a resolution of $\mathbb{Z}$ that naturally involves functions on $G^n = G \times G \times G \times \cdots \times G$.

The idea is to look at a sequence like

$$(\dagger) \qquad \cdots \xrightarrow{d_3} \mathrm{Fun}'(G^3,\mathbb{Z}) \xrightarrow{d_2} \mathrm{Fun}'(G^2,\mathbb{Z}) \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

We define a $\mathbb{Z}[G]$-module structure on $P_n = \mathrm{Fun}'(G^{(n+1)},\mathbb{Z})$ by setting $g\cdot[(g_0,g_1,g_2,g_3,\ldots,g_n)] = [(gg_0,gg_1,gg_2,gg_3,\ldots,gg_n)]$ for $g \in G$ and $(g_1,g_2,\ldots,g_n) \in G^n$.

(387) Verify that P_n is a free $\mathbb{Z}[G]$-module.

The map ε occurring in the complex (†) is the augmentation map. On basis vectors, we have $d_1([(g_0,g_1)]) = [g_0] - [g_1]$, $d_2([(g_0,g_1,g_2)]) = [(g_1,g_2)] - [(g_0,g_2)] + [(g_0,g_1)]$, and

$$d_n([(g_0,g_1,\ldots,g_n)]) = \sum_{j=0}^{n} (-1)^j [(g_0,g_1,\ldots,\widehat{g_j},\ldots g_n)].$$

(388) Verify that (†) is exact at P_1, $\mathbb{Z}[G]$, and $\mathbb{Z}$.

(389) (*Bonus.*) Show that † is a complex.

(390) (*Bonus.*) Show that † is exact. [Hint: for $m \geq 1$ define $h_m\colon P_m \to P_{m+1}$ on basis elements by $h([(g_0,g_1,\ldots,g_m)] = [(s,g_0,g_1,\ldots,g_m)]$. Check that $d_{m+1}h_m + h_{m-1}d_m = \mathrm{Id}_{P_m}$.]

[1] So called because if G acts trivially on A, then f is a true homomorphism.

Please report any errors you find to smdbackr@umich.edu

Suppose M is a $\mathbb{Z}[G]$-module. Applying the functor $M \mapsto \mathrm{Hom}_{\mathbb{Z}[G]}(\cdot, M)$ to the appropriate deleted complex we arrive at the complex

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \xrightarrow{d_1^*} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^2, \mathbb{Z}), M) \xrightarrow{d_2^*} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^3, \mathbb{Z}), M) \xrightarrow{d_3^*} \cdots$$

(391) Show that $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^{m+1}, \mathbb{Z}), M)$ can be identified with those elements $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Fun}'(G^{m+1}, \mathbb{Z}), M)$ that satisfy

(*) $$f(gg_0, gg_1, \ldots, gg_m) = g \cdot f(g_0, g_1, \ldots, g_m).$$

(392) Show that a function $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Fun}'(G^{m+1}, \mathbb{Z}), M)$ that satisfies (*) is completely determined by its values at elements of G^m of the form $(e, y_1, y_1y_2, y_1y_2y_3, \ldots, y_1y_2y_3 \cdots y_m)$.

If we define

$$\varphi(x_1, x_2, \ldots, x_m) = f(e, x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2x_3 \cdots x_m),$$

then $\delta^*\varphi(z_1, z_2, \ldots, z_m, z_{m+1})$ is

$$z_1 \cdot \varphi(z_2, z_3, \ldots, z_{m+1}) + \sum_{j=1}^{m} (-1)^j \varphi(z_1, z_2, \ldots z_{j-1}, z_jz_{j+1}, z_{j+2} \ldots, z_{m+1}) + (-1)^{m+1}\varphi(z_1, z_2, \ldots, z_m)$$

Important: We are identifying $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^{m+1}, \mathbb{Z}), M)$ with functions of m-variables, so the δ^* above corresponds to the map d_{m+1}^* from $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^{m+1}, \mathbb{Z}), M)$ to $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Fun}'(G^{m+2}, \mathbb{Z}), M)$.

(393) (*Bonus*) Prove that the formula for δ^* is correct.

(394) Describe $\mathrm{H}^j(G, M)$ for $j \in \{0, 1, 2\}$. [Your answer will be in terms of cycles and coboundaries.]

Something to Think About

It is rare to see an $H^3(G, M)$ in the wild. In practice, it is enough to have a good understanding of how to calcuate $\mathrm{H}^j(G, M)$ for $j \in \{0, 1, 2\}$.

That said, it is pretty common to be in a situation where G is acting on something more exotic than an abelian group. For example, the group $\mathbb{Z}/(2)$ acts on $\mathbb{C}$ via conjugation, hence it acts on natural $\mathbb{C}$-objects like $\mathrm{SL}_2(\mathbb{C})$ that are not abelian.

Here is a typical example from the wild. Let $X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and let $\mathcal{O}(\mathbb{C}) = {}^{\mathrm{SL}_2(\mathbb{C})} X$; the $\mathrm{SL}_2(\mathbb{C})$-orbit of X under conjugation. The centralizer, let us call it $U(\mathbb{C})$, of X in $\mathrm{SL}_2(\mathbb{C})$ consists of all matrices of the form $\begin{bmatrix} \pm 1 & x \\ 0 & \pm 1 \end{bmatrix}$ with $x \in \mathbb{C}$. We have an exact sequence of "complex objects"

$$0 \longrightarrow U(\mathbb{C}) \longrightarrow \mathrm{SL}_2(\mathbb{C}) \longrightarrow \mathcal{O}(\mathbb{C}) \longrightarrow 0.$$

When we take $\mathbb{Z}/(2)$ fixed points, we get

$$0 \longrightarrow U(\mathbb{R}) \longrightarrow \mathrm{SL}_2(\mathbb{R}) \longrightarrow \mathcal{O}(\mathbb{R})$$

and this is not right exact because, for example, $\mathcal{O}(\mathbb{R})$ contains the element $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, which is not $\mathrm{SL}_2(\mathbb{R})$-conjugate to X. Any thoughts on how to proceed?

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 0b (Due September 10, a Monday!)
(This is much longer than a usual Monday homework.)

(1) (*) The Kuratowski-Zorn lemma will be used freely in this class. There is no assumption that you have seen it or its many equivalent formulations before. Please familiarize yourself with it (see, for example, [DF04, pp. 907–909]).
(2) Fix a prime p. Consider the subset $A \subset \mathbb{Q}$ consisting of those $q \in \mathbb{Q}$ that can be expressed as a/b with $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus p\mathbb{Z}$. Is A a ring (with respect to the usual operations on $\mathbb{Q}$)? [$\mathbb{Z} \setminus p\mathbb{Z}$ is the complement of $p\mathbb{Z}$ in $\mathbb{Z}$.]
(3) Basics of vector spaces.
  (a) If F is a field, then F^n and $F[x]$ are examples of F-vector spaces. Give six examples of vector spaces that are more interesting than the two already given.
  (b) Suppose F is a field and V an F-vector space. Let 0_F and 0_V denote the additive identities of F and V, respectively. Verify the following statements.
    (i) For all $a \in F$ we have $a0_V = 0_V$.
    (ii) For all $v \in V$ we have $0_F v = 0_V$.
    (iii) For all $v \in V$ we have $(-1)v = -v$.
    (iv) If $a \in F$ and $v \in V$ such that $av = 0_V$, then $a = 0_F$ or $v = 0_V$.
  (c) Recall the definitions of words like *linearly dependent*, *span*, *linear combination*, *linearly independent*, *basis*, *linear transformation*, *subspace*, etc.
  (d) What is $\operatorname{span}(\emptyset)$? What is $\dim(\{0\})$? Is the empty set linearly independent? What is a basis for $\{0\}$? If a list of vectors contains 0, can it be linearly independent? How many two-dimensional subspaces are in $\mathbb{R}^3$? How many two-dimensional subspaces are in F^3 if F is a finite field with q elements?
(4) Some problems about linear independence (and a little bit of span).
  (a) Show that the list $T = (\sin(nt) \mid n \in \mathbb{N})$ is a linearly independent list of $C^\infty((-\pi, \pi))$.
  (b) Suppose F is a field and V is an F-vector space. An indexed list $S \subset V$ is linearly independent if and only if for all finite sublists $A \subset S$ we have that A is linearly independent.
  (c) Suppose F is a field and V is an F-vector space. Suppose $S \subset V$ is a linearly independent set and $w \in V \setminus S$. Exactly one of the following is true: Either $S \cup \{w\}$ is linearly independent or $w \in \operatorname{span}(S)$.
  (d) Suppose F is a field and V is an F-vector space. Let $S_n = (v_1, v_2, v_3, \ldots, v_n)$ be a linearly dependent list of vectors in V . Show there is a smallest $j \leq n$ such that v_j is a linear combination of elements of $S_{j-1} = (v_1, v_2, \ldots, v_{j-1})$.
(5) Some problems about span. Suppose F is a field and V is an F-vector space.
  (a) If $X \subset V$, then $\operatorname{span}(X)$ is a subspace of V.
  (b) Show that if $X \subset Y \subset V$, then $\operatorname{span}(X)$ is a subspace of $\operatorname{span}(Y)$.
  (c) If W is a subspace of V, then $\operatorname{span}(W) = W$.
  (d) If $X \subset V$, then $\operatorname{span}(\operatorname{span}(X)) = \operatorname{span}(X)$.
  (e) Let X, Y, Z be subsets of V. If $Y \subset \operatorname{span}(X)$ and $Z \subset \operatorname{span}(Y)$, then $Z \subset \operatorname{span}(X)$.
(6) Suppose F is a field and V is an F-vector space. Show that for any indexed list $S \subset V$ the following are equivalent.
  (a) S is a maximal linearly independent subset of V.
  (b) S is a basis for V.
  (c) S is a minimal spanning set of V.
(7) Suppose F is a field and V is an F vector space. Suppose X, Y are finite subsets of V with $X \subset Y$, X is linearly independent, and Y spans V. Show that there exists a basis B of V such that $X \subset B \subset Y$.
(8) Suppose F is a field and V is an F-vector space. Suppose $X = (x_1, x_2, \ldots, x_n) \subset V$ is a finite and linearly independent list of vectors and suppose $Y = (y_i \mid i \in I) \subset V$ spans V. Here I is an indexing set. Then there is an injective function $f \colon \mathbb{N}_n = \{1, 2, 3, \ldots, n\} \to I$ such that $X \cup (y_i \mid i \in I \setminus f(\mathbb{N}_n))$ spans V.
(9) On dimension. Suppose F is a field and V is an F-vector space.
  (a) Let $S, B \subset V$ be finite lists of vectors.
    (i) Suppose B is linearly independent. If $|S| < |B|$, then S does not span V.
    (ii) Suppose B spans V. If $|S| > |B|$, then S is not linearly independent.
  (b) If V admits a finite basis, then all bases of V have the same cardinality. (This is why the definition of the dimension of a vector space makes sense.)
  (c) If W is a subspace of V and V is finite dimensional, then any basis of W may be extended to a basis of V.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 1a (Due September 14)

(10) (*) Suppose G is a finite cyclic group and $d \in \mathbb{N}$ divides $|G|$, the order of G. Show that there are exactly d elements in G whose order divides d.

(11) (*) What are the subgroups of $\mathbb{Z}$?

(12) (*) Suppose G and H are groups and $\varphi\colon G \to H$ is a group homomorphism. Show that $\ker(\varphi)$ is a normal subgroup of G and $G/\ker(\varphi)$ is isomorphic to $\mathrm{im}(\varphi)$ as groups.

(13) (*) Suppose G is a group and H, K are normal subrgoups of G with $H \leq K$. Show that K/H is a normal subgroup of G/H and $(G/H)/(K/H)$ is isomorphic to G/K as groups.

(14) (*) Suppose S is a finite set and $f\colon S \to S$. Show that the following are equivalent.
- f is injective.
- f is surjective.
- f is bijective. [That is, f is an isomorphism in the category of sets.]

(15) (*) Suppose R is a ring. Is every R-module also a ring?

(16) (*) Suppose R is a commutative ring. Show that $R[x_1, x_2, \ldots, x_n]$, the set of polynomials in indeterminates $x_1, x_2, \ldots, x_n$ and coefficients in R, is a commutative ring where multiplication is given by $(fg)(x) = f(x)g(x)$.

(17) (*) Suppose R is a commutative ring. The polynomial algebra $R[x_1, x_2, \ldots, x_n]$ with multiplication given by $(fg)(x) = f(x)g(x)$ is an associative, commutative algebra.

(18) (*) Suppose A is an R-algebra. Is A also a ring? Is A a module over the ring R?

(19) (*) Suppose R is a ring and $a, b \in R$. Show: If $b \in R^\times$ and $a \mid b$, then $a \in R^\times$.

(20) Suppose k is a field.
- (a) Suppose V is a k-vector space and $T \in \mathrm{End}_k(V)$. Show that V is a $k[x]$-module where $pv = p(T)v$ for $p \in k[x]$ and $v \in V$.
- (b) Show that if M is a $k[x]$-module, then M is a k-vector space and there exists $T \in \mathrm{End}_k(V)$ so that for $p \in k[x]$ and $v \in V$ we have $pv = p(T)v$.
- (c) Conclude that modules over $k[x]$ are parameterized by pairs (V, T) where V is a k-vector space and $T \in \mathrm{End}_k(V)$.

Definition. Suppose A is a $\mathbb{Z}$-module (that is, A is an abelian group). An element $a \in A$ is called a *torsion element* of A provided that there exists a nonzero $m \in \mathbb{Z}$ for which $ma = 0$. The set of torsion elements in A is denoted $\mathrm{Tor}(A)$ or A_{tor}. The abelian group A is said to be a *torsion group* provided that $A = A_{\text{tor}}$. If $A_{\text{tor}} = \{0\}$, then A is said to be *torsion free*.

(21)
- (a) Suppose that A is a $\mathbb{Z}$-module. Show that A_{tor} is a subgroup of A; it is called the *torsion subgroup of* A.
- (b) Suppose that A is a $\mathbb{Z}$-module. Show that A/A_{tor} is torsion free.
- (c) Describe $(\mathbb{Z}[x]/(x^2+1))_{\text{tor}}$.
- (d) Show that the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a torsion group.

(22) (*) Suppose R is a commutative ring.
- (a) Show that A is an associative[1] R-algebra with identity[2] if and only if A is a ring together with a ring map $R \to A$ whose image is contained in the center of A.
- (b) Suppose A_1 and A_2 are two associative R-algebras. Show that $f \in \mathrm{Hom}_{R-alg}(A_1, A_2)$ if and only if f is a ring map that commutes with the maps of R to each A_i.

(23) Suppose that R is a ring.
- (a) Show there is a unique ring homomorphism $f\colon \mathbb{Z} \to R$. [Hint: for uniqueness, note that $f(0) = f(0+0)$.]
- (b) The kernel of f is a subgroup of $\mathbb{Z}$, hence of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. We define the *characteristic of* R to be n. Show that if R is a field, then n is a prime number or zero.
- (c) (*Bonus*) Show that every ring is naturally an associative $\mathbb{Z}$-algebra.

(24) Suppose R is a commutative ring. Let $\mathrm{Bil}(M \times N, P)$ denote the R-bilinear maps from $M \times N$ to P. Show that $\mathrm{Bil}(M \times N, P)$ is an R-module where $r \in R$ acts on $B \in \mathrm{Bil}(M \times N, P)$ by $(rB)(a, b) = B(ra, b) = B(a, rb)$. What can you say about $\mathrm{Bil}(M \times N, P)$ if R is not commutative?

(25) (*) Show that $\mathrm{Mat}_n(\mathbb{Q})$ with multiplication defined by $[A, B] = AB - BA$ is a $\mathbb{Q}$-algebra that is neither associative nor commutative.

[1] That is, the bilinear map $A \times A \to A$ is associative.

[2] That is, the bilinear map $A \times A \to A$ admits an identity.

(26) Suppose that R is a ring.
  (a) If I is a an ideal[1] in R, show that R/I is naturally a ring, called the quotient ring.
  (b) (First Isomorphism Theorem.) Show that if R and S are rings and $\sigma\colon R \to S$ is a ring homomorphism, then $R/\ker(\sigma)$ is isomorphic (in the category of rings) to $\mathrm{im}(\sigma)$.
  (c) Conclude that if σ is surjective, then $R/\ker(\sigma) \simeq S$.

(27) What is the cardinality of the following rings.
  (a) $\mathbb{Z}[x]/(6, 2x-1)$.
  (b) $\mathbb{Z}[x]/(x^2-3, 2x+4)$.

(28) Suppose R is a nonzero ring. An element $e \in R$ is called *idempotent* if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(e-1)$ are two sided ideals of R and that $R \simeq Re \times R(1-e)$. Show that e and $(1-e)$ are identities for the subrings Re and $R(1-e)$, respectively.

(29) Let R be a ring. Suppose $I, J \subset R$ are ideals. Show that $I \cup J$ is an ideal if and only if $I \subset J$ or $J \subset I$.

Definition. A *category* $\mathcal{C}$ consists of a class of objects, $\mathrm{Ob}(\mathcal{C})$, and sets of morphisms between those objects. For every ordered pair of objects A, B in $\mathrm{Ob}(\mathcal{C})$ there is a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of morphisms from A to B, and for every ordered triple A, B, C in $\mathrm{Ob}(\mathcal{C})$ there is a law of composition of morphisms

$$\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C).$$

For $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ we write gf for the image of (f, g) in $\mathrm{Hom}_{\mathcal{C}}(A, C)$. The objects and morphisms of $\mathcal{C}$ satisfy the following axioms:

C1: the composition of morphisms is associative;
C2: for each object C in $\mathcal{C}$ there is an identity morphism, $\mathrm{Id}_C \in \mathrm{End}_{\mathcal{C}}(C) := \mathrm{Hom}_{\mathcal{C}}(C, C)$;
C3: for every ordered pair A, B in $\mathrm{Ob}(\mathcal{C})$ we have $f \,\mathrm{Id}_A = f$ and $\mathrm{Id}_B \, f = f$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$; and
C4: if A, B, C, D in $\mathrm{Ob}(\mathcal{C})$ and $A \neq C$ or $B \neq D$, then $\mathrm{Hom}_{\mathcal{C}}(A, B)$ and $\mathrm{Hom}_{\mathcal{C}}(C, D)$ are disjoint sets.

(30) (*) Show that the category of rings, the category of modules, and the category of algebras are all categories.

(31) Suppose k is a field. Let $\mathcal{C}$ denote the collection of pairs (V, T) where V is a k-vector space and $T \in \mathrm{Hom}_k(V, V)$. Show that if we declare that a morphism between two pairs (V_1, T_1) and (V_2, T_2) is a map $\varphi \in \mathrm{Hom}_k(V_1, V_2)$ satisfying $\varphi \circ T_1 = T_2 \circ \varphi$, then $\mathcal{C}$ is a category.

(32) Let R be a ring. For $r \in R$ and $1 \leq i \neq j \leq n$ define the $n \times n$ matrix $E(i, j, r)$ by

$$E(i,j,r)_{k\ell} = \begin{cases} 1 & \text{if } k = \ell, \\ r & \text{if } k = i \text{ and } j = \ell, \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

Suppose X is an $m \times n$ matrix. What is the effect of right multiplication by $E(i, j, r)$ on X? Suppose Y is an $n \times m$ matrix. What is the effect of left multiplication by $E(i, j, r)$ on Y? What is the inverse of $E(i, j, r)$?

(33) Let R be a ring. For $r \in R^\times := \{x \in R \,|\, \exists s \in R \text{ for which } xs = sx = 1\}$ and $1 \leq i \leq n$ define the $n \times n$ matrix $E(i, r)$ by

$$E(i,r)_{k\ell} = \begin{cases} 1 & \text{if } k = \ell \neq i, \\ r & \text{if } k = \ell = i, \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

Suppose X is an $m \times n$ matrix. What is the effect of right multiplication by $E(i, r)$ on X? Suppose Y is an $n \times m$ matrix. What is the effect of left multiplication by $E(i, r)$ on Y? What is the inverse of $E(i, r)$?

(34) Let R be a ring. For $1 \leq i < j \leq n$ define the $n \times n$ matrix $E(i, j)$ by

$$E(i,j)_{k\ell} = \begin{cases} 1 & \text{if } k = \ell \notin \{i, j\}, \\ 1 & \text{if } \{k, \ell\} = \{i, j\}, \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

Suppose X is an $m \times n$ matrix. What is the effect of right multiplication by $E(i, j)$ on X? Suppose Y is an $n \times m$ matrix. What is the effect of left multiplication by $E(i, j)$ on Y? What is the inverse of $E(i, j)$?

[1] Recall that "ideal" means "two-sided ideal."

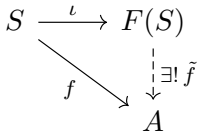
Please report any errors you find to smdbackr@umich.edu

I will assume that you are familiar with the idea of a free abelian group on a set S. If your undergraduate abstract algebra class did not cover this concept, then here is a crash course. We will denote a free abelian group on a set S by $F(S)$. As a set, the elements of $F(S)$ are the formal $\mathbb{Z}$-linear finite combinations of elements of S. That is

$$n_1 s_1 + n_2 s_2 + \cdots + n_\ell s_\ell$$

where $n_1, n_2, \ldots, n_\ell \in \mathbb{Z}$, $s_1, s_2, \ldots s_\ell \in S$ and $\ell \in \mathbb{N}$. By convention $F(\emptyset) = \{0\}$. The product of two elements in $F(S)$ is given by component wise addition of the coefficients. If S has finite cardinality, say $|S| = m$, then $F(S)$ is isomorphic, as a group, to $\mathbb{Z}^{\oplus m} = \bigoplus_{i=1}^{m} \mathbb{Z}$, the direct sum of m copies of $\mathbb{Z}$. A "$\mathbb{Z}$-algebra presentation" of an algebra means a set of generators and relations for the algebra. For example, a $\mathbb{Z}$-algebra presentation of the Gaussian integers $\mathbb{Z}[i]$ is $\mathbb{Z}[x]/(x^2+1)$. Free abelian groups satisfy the following universal property:

Universal Property of free abelian groups. Suppose S is a set. A *free abelian group* with basis S is an abelian group, denoted $F(S)$ or $F^{\text{ab}}(S)$, together with an injection $\iota\colon S \to F(S)$ such that for every abelian group A and every (set) function $f\colon S \to A$ there exists a unique group homomorphism $\tilde{f}\colon F(S) \to A$ for which the following diagram commutes.



(35) Show that a free abelian group with basis S is unique up to unique isomorphism.
(36) (*) Describe $\mathbb{Z}[x]/(x^2-2)$
(37) Show that $F(\mathbb{N}) \simeq F(\mathbb{N} \times \mathbb{N})$ as abelian groups. Is it true that $F(\mathbb{N}) \simeq F(\mathbb{N}) \times F(\mathbb{N})$?
(38) Suppose A and B are finite sets. Show that $F(A) \simeq F(B)$ as abelian groups if and only if $A \simeq B$ as sets. [Hint: From linear algebra you know that two k-vector spaces are isomorphic iff they have the same dimension.] *Bonus*. Show the result is valid without the assumption that A and B are finite.

If you have never dealt with exact sequences before, it is time to start. If you have, help your peers.

(39) (*) Suppose R is a ring, M_1, M_2, M_3 are R-modules, and $d_i \in \text{Hom}_R(M_i, M_{i-1})$. Show that $d_i \circ d_{i+1} = 0$ is equivalent to $\text{im}(d_{i+1}) \subset \ker(d_i)$.

Definition. Suppose R is a ring. A *chain complex of R-modules* is a sequence of R-modules and R-module homomorphisms

$$\cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

such that $d_i \circ d_{i+1} = 0$ for all i. The sequence is said to be *exact at* M_i provided that $\text{im}(d_{i+1}) = \ker(d_i)$. The sequence is said to be *exact* provided that it is exact at M_i for all i.

(40) (*) Show that a complex

$$\cdots \longrightarrow 0 \longrightarrow L \xrightarrow{\alpha} M \longrightarrow \cdots$$

is exact at L if and only if α is injective.
(41) (*) Show that a complex

$$\cdots \longrightarrow M \xrightarrow{\beta} N \longrightarrow 0 \longrightarrow \cdots$$

is exact at N if and only if β is surjective.
(42) In the notation of Homework 26: Show that if σ is surjective, then the sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \ker(\sigma) \longrightarrow R \xrightarrow{\sigma} S \longrightarrow 0$$

is exact. This is an example of a *short exact sequence*. In fact, it is a short exact sequence of R-modules; explain.

Math 593. Homework 1b (Due September 17)

(43) Suppose F is a field and V, W are F-vector spaces.
  (a) Show that $\text{Hom}_F(V, W)$ is an F-vector space.

(b) If $T \in \mathrm{Hom}_F(V,W)$, then $\mathrm{im}(T)$, the image of T, is a subspace of W and $\ker(T)$, the kernel of T, is a subspace of V.

(c) If $S \in \mathrm{Hom}_F(V,W)$ is injective, then there exists $R \in \mathrm{Hom}_F(\mathrm{im}(S), V)$ such that $R \circ S(v) = v$ for all $v \in V$.

(d) If $T \in \mathrm{Hom}_F(V,W)$ is injective, then the image of every linearly independent list of vectors is linearly independent.

(e) As a sort of converse to the above statement, we have: Suppose $T \in \mathrm{Hom}_F(V,W)$ and B is a basis for V. If $T(B)$ is linearly independent in W, then T is injective.

(f) If V is finite dimensional and $T \in \mathrm{Hom}_F(V,W)$, then

$$\dim(V) = \dim(\ker(T)) + \dim(\mathrm{im}(T)).$$

(44) Suppose V and W are finite dimensional F-vector spaces with $\dim(V) = \dim(W)$. Suppose $T \in \mathrm{Hom}_F(V,W)$. The following are equivalent:

♡ T is injective.

♢ T is surjective.

♠ T is an isomorphism.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 2a (Due September 21)

(45) (*) Suppose k is a field and $p \in k[x]$ is a polynomial of degree $m > 0$. Show that p has at most m roots in k. [This is true even if we count with multiplicity.]

(46) (*) Suppose R is a ring. Show that R has a maximal ideal.

(47) Suppose R is a nonzero commutative ring and $I \subset R$ is an ideal. The following results characterize prime and maximal ideals in terms of their respective quotients.
  (a) (*) Show that R is a field if and only if the only possibilities for I are $\{0\}$ or R.
  (b) Show that I is a maximal ideal if and only if R/I is a field. [Hint: Use Homework 47a. In R/I choose and ideal $0 \neq J \subset R/I$. Define $S = \{r \in R \,|\, r + I \subset J\}$.]
  (c) (*) Show that I is a prime ideal if and only if R/I is an integral domain.
  (d) (*) Conclude that every maximal ideal of a nonzero commutative ring is a prime ideal.

(48) (*) Suppose R is a domain and $a, b, c \in R$ with $a \neq 0$. Show that if $ab = ac$, then $b = c$.

(49) (*) Suppose R is a ring. Show that R is a domain if and only if 0 is the only left zero divisor.

(50) (*) Let R be the subring of $\mathbb{Q}[x]$ consisting of polynomials with integer constant coefficient. Show that R is an integral domain, but it is not Noetherian. [Hint: Let $I_n = (x/43^n)$; this example shows that, in fact, not all rings satisfy the ascending chain condition for principal ideals.]

(51) (*) Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-13}]$. Consider the ideal I generated by 7 and $6 + \sqrt{-13}$. Show that I is not principal. [Hint: This is very similar to [DF04, Example 2, p. 273].]

(52) (*) Suppose R is an integral domain.
  (a) Show that $R[x]$ is an integral domain.
  (b) if $D = R \setminus \{0\}$, then the localization of R at D is called the *field of fractions* or *quotient field* of R. Show that this name is deserved; that is, show $D^{-1}R$ is a field.

(53) (*) Suppose R is a commutative ring and $I \subset R$ is an ideal. Show that $R \setminus I$ is multiplicative if and only if I is a prime ideal.

Definition. Suppose A is a commutative ring and $a, b \in A$ with $b \neq 0$. A *greatest common divisor* or *gcd* of a and b is a nonzero $d \in A$ for which
- $d \mid a$ and $d \mid b$ and
- if $d' \in A$ divides both a and b, then $d' \mid d$.

(54) (*) Suppose that A is a commutative ring and d is a gcd of $a, b \in A$. Show that (d) is the smallest principal ideal containing a and b.

(55) (*) Suppose that A is an integral domain. Show that if $d, d' \in A$ with $(d) = (d')$, then there is a unit $u \in A^\times$ for which $d = ud'$. Conclude that the gcd of a and b in A is unique up to units.

Definition. Suppose R is a ring. An element $x \in R$ is said to be *nilpotent* provided that $x^n = 0$ for some $n \in \mathbb{N}$.

(56) (*) Suppose that R is a ring and $x \in R$ is nilpotent. Show: $(1 + x) \in R^\times$.

(57) Suppose R is a ring.
  (a) Suppose $a, b \in R$ with $ab = ba$. Show that if a and b are nilpotent, then $a + b$ is nilpotent. Is this true if a and b do not commute?
  (b) Show that if R is commutative, then the set of nilpotent elements in R form an ideal; it is called the *nilradical of* R and often denoted $\mathrm{Nil}(R)$.
  (c) Suppose R is commutative and $D \subset R$ is multiplicative. Show that $D^{-1}R$ is the zero ring if and only if $D \cap \mathrm{Nil}(R) \neq \emptyset$.

(58) (*) Suppose that S is a set and R is a ring. Let $\mathrm{Fun}'(S, R)$ be the set of functions $f \colon S \to R$ for which $f(s) = 0$ for all but finitely many $s \in S$. Show that with respect to pointwise addition of functions and pointwise multiplication of ring elements, $\mathrm{Fun}'(S, R)$ is an R-module.

(59) Suppose R is a ring. Show that the following statements are equivalent.
  (a) Every nonempty set of left ideals in R has a maximal element (with respect to inclusion).
  (b) If $I \subset R$ is a left ideal, then there exist $r_1, r_2, \ldots r_k \in R$ for which $I = (r_1, r_2, \ldots, r_k)$.
  (c) R is Noetherian.

(60) Suppose p is a prime, and let $\mathbb{Z}_{(p)}$ denote the localization of $\mathbb{Z}$ at p. The map $\nu = \nu_p \colon \mathbb{Z}_{(p)} \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ defined by $\nu(x) = n$ provided that $x \in p^n\mathbb{Z}_{(p)} \setminus p^{n+1}\mathbb{Z}_{(p)}$ is called a discrete valuation. Show:
  (a) ν is surjective.
  (b) $\nu(ab) = \nu(a) + \nu(b)$ for all $a, b \in \mathbb{Z}_{(p)}^{\times}$.
  (c) $\nu(a+b) \geq \min(\nu(a), \nu(b))$ for all $a, b \in \mathbb{Z}_{(p)} \setminus \{0\}$ with $a + b \neq 0$.
  (d) Show that $\mathbb{Z}_{(p)}$ is a Euclidean Domain. [Hint: ν is almost a positive norm.]

(61) (*) Understanding how the Euclidean Algorithm works is pretty important, so do this exercise by hand (or, if you use a computer, you must program the computer yourself). For each of the following pairs of integers a and b, determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.
  (a) $a = 21, b = 34$
  (b) $a = 11391, b = 5673$
  (c) $a = 91442056588823, b = 779086434385541$

(62) (*) Understanding how the Euclidean Algorithm works is pretty important, so do this exercise by hand (or, if you use a computer, you must program the computer yourself). For each of the following pairs of Gaussian integers a and b, determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.
  (a) $a = 85, b = 1 + 13i$
  (b) $a = 47 - 13i, b = 53 + 56i$

(63) Suppose R is a ring and $A \subset R$ is a subring that contains the multiplicative idenity element of R. Suppose I is an ideal in R. Show that $A + I$ is a subring of R, $A \cap I$ is an ideal of A, and $(A + I)/I$ is isomorphic to $A/(A \cap I)$ as rings.

(64) Suppose R is a UFD and $a, b \in R[x]$. If the gcd of the coefficients of a is one and the gcd of the coefficients of b is one, what can you conclude about the gcd of the coefficients of ab? What about the converse: if the gcd of the coefficients of ab is one, what can you conclude about the gcd of the coefficients of a (resp. b)? [Hint: If your solution requires that you write out polynomials, then you are not using the full suite of tools at your disposal.]

Definition. Suppose R is a commutative ring and $0 \neq c \in R \setminus R^{\times}$. We say that c *factors in* R provided that there exists $a, b \in R$ for which $c = ab$ and neither a nor b is a unit.

(65) Factoring is a common way to discuss the notion of irreducibility.
  (a) Suppose R is a commutative ring and $d \in R$ is a non-zero non-unit. Show that d does not factor in R if and only if d is irreducible.
  (b) **Warning:** the notions of irreducible and factoring are **very**[1] dependent on the underlying ring. Does $7x$ factor in $\mathbb{Z}[x]$? Does it factor in $\mathbb{Q}[x]$? Does $6x^2 + 9x + 18$ factor in $\mathbb{Z}[x]$? Does it factor in $\mathbb{Q}[x]$?

(66) Let R be an integral domain. R is said to have the Bezout Property provided that every ideal in R that is generated by two elements is a principal ideal.
  (a) Prove that R has the Bezout Property if and only if every pair of elements $a, b \in R$ has a gcd d that can be written as $d = az + by$ for some $x, y \in R$. [Thus, an example of an integral domain for which the Bezout Property fails is the ring of polynomials in two variables s and t: $\gcd(st, s2 + st) = s$, but the equation $stx + (s2 + st)y = s$ has no solutions for (x, y).]
  (b) Prove that if R has the Bezout Property, then every finitely generated ideal of R is a principal ideal. [Warning: there exist integral domains with the Bezout Property which are NOT PIDs. See [DF04, Exercise 12, p. 302].]

(67) Let E be any of the three types of matrices defined in Exercises 32, 33, or 34. Right multiplication by E is called an *elementary column operation* (ECO) and left multiplication by E is called an *elementary row operation* (ERO). Computationally, EROs and ECOs are very useful in pretty much every branch of mathematics.
  (a) If $Q \in \mathrm{End}_R(R^n)^{\times}$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is a basis for R^n, then $Q\mathbf{v} = (Qv_1, Qv_2, \ldots, Qv_n)$ is a basis for R^n. What does this say about bases and elementary matrix operations?
  (b) If $T \in \mathrm{Hom}_R(R^n, R^m)$ and $S \in \mathrm{End}_R(R^m)^{\times}$, then $\ker(T) = \ker(S \circ T)$. What does this say about kernels and elementary matrix operations?

(68) Suppose A is a $\mathbb{Z}$-module. For $m \in \mathbb{N}$ let ${}_mA = \{a \in A \,|\, ma = 0\}$.
  (a) Is ${}_mA$ a subgroup of A?
  (b) Describe ${}_m(\mathbb{Q}/\mathbb{Z})$.
  (c) Show that $A = \bigcup_{m \in \mathbb{N}} {}_mA$ if and only if A is a torsion group.

[1] This is why, when discussing polynomials, words like primitive and nonconstant are forever appearing in discussions of irreducibility.

(69) Suppose R is an commutative ring. If $R[x]$ is a PID, then R is a field. [Hint: Every PID is an integral domain.]

(70) EROs and ECOs: Smith Normal Form over $\mathbb{Z}$ for small matrices.[1]

(a) Suppose that A is a 2×2 matrix with entries in $\mathbb{Z}$. Show that there are elementary matrices $E_1, E_2, \ldots, E_r$ and $F_1, F_2, \ldots, F_c$ with entries in $\mathbb{Z}$ so that $B = E_r \cdot E_{r-1} \cdots E_2 \cdot E_1 \cdot A \cdot F_1 \cdot F_2 \cdots F_{c-1} \cdot F_c$ has the form

$$\begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix}$$

with $b_{ii} \in \mathbb{Z}$ and $b_{11} \mid b_{22}$. It turns out, as we shall see later, that B is unique (up to units, which in this case are ± 1) and is called the Smith Normal Form of A.

(b) Suppose that A is a 3×3 matrix with entries in $\mathbb{Z}$. Show that there are elementary matrices $E_1, E_2, \ldots, E_r$ and $F_1, F_2, \ldots, F_c$ with entries in $\mathbb{Z}$ so that $B = E_r \cdot E_{r-1} \cdots E_2 \cdot E_1 \cdot A \cdot F_1 \cdot F_2 \cdots F_{c-1} \cdot F_c$ has the form

$$\begin{pmatrix} b_{11} & 0 & 0 \\ 0 & b_{22} & 0 \\ 0 & 0 & b_{33} \end{pmatrix}$$

with $b_{ii} \in \mathbb{Z}$ and $b_{11} \mid b_{22} \mid b_{33}$. It turns out, as we shall see later, that B is unique (up to units, which in this case are ± 1) and is called the Smith Normal Form of A.

(c) Compute the Smith Normal Form of

$$\begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix} \text{ and } \begin{pmatrix} 9 & 5 & 7 \\ -9 & -6 & 9 \\ -3 & -2 & -1 \end{pmatrix}.$$

(71) In the ring $\mathbb{Z}[\sqrt{-13}]$ show that 2, 7, $1 + \sqrt{-13}$ and $1 - \sqrt{-13}$ are irreducible. Which are prime?

Definition. Suppose R is a ring. A *short exact sequence of R-modules* is an exact sequence of the form

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

We say that M is an *extension of N by L*.

(72) Suppose $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ is a short exact sequence of R-modules. Show that $N \simeq M/\ker(\beta) \simeq M/\operatorname{im}(\alpha)$.

(73) (*) Suppose X, Y are R-modules and $f \in \operatorname{Hom}_R(X, Y)$. Create a short exact sequence from X, $\ker(f)$, and $\operatorname{im}(f)$.

Definition. Suppose $\mathcal{D}$ is a category. A *subcategory* $\mathcal{C}$ of $\mathcal{D}$ is a category for which every object of $\mathcal{C}$ is an object in $\mathcal{D}$ and for every ordered pair A, B of objects in $\mathcal{C}$ we have $\operatorname{Hom}_{\mathcal{C}}(A, B) \subset \operatorname{Hom}_{\mathcal{D}}(A, B)$. We say that $\mathcal{C}$ is a *full subcategory* of $\mathcal{D}$ provided that $\mathcal{C}$ is a subcategory of $\mathcal{D}$ and for every ordered pair A, B of objects in $\mathcal{C}$ we have $\operatorname{Hom}_{\mathcal{C}}(A, B) = \operatorname{Hom}_{\mathcal{D}}(A, B)$.

(74) (*) Show that the category of fields is a full subcategory of the category of commutative rings.

Math 593. Homework 2b (Due September 24)

(75) Suppose that F is a field and V is an n-dimensional F-vector space. We also assume that F doesn't have characteristic two. Suppose $f\colon V \times V \times \cdots \times V \times V \to F$ is a function (there are d copies of V here). The function f is called *multilinear* provided that it is linear in each variable (for fixed values of the remaining variables). The space of multilinear functions on V in d variables with values in F is denoted $\operatorname{Mult}^d(V, F)$. A function in $\operatorname{Mult}^d(V, F)$ is called *alternating* provided that $f(v_1, v_2, \ldots, v_d) = 0$ whenever there exists $i \neq j$ such that $v_i = v_j$. It is called *skew-symmetric* provided that switching two entries results in a change of sign.

(a) Show that a function $f \in \operatorname{Mult}^d(V, F)$ is skew-symmetric if and only if it is alternating.

(b) The subset of alternating functions in $\operatorname{Mult}^d(V, F)$ is denoted $\operatorname{Alt}^d(V, F)$. Show that $\operatorname{Alt}^d(V, F)$ is a vector space.

(c) Show that for $d > n$ we have $\dim(\operatorname{Alt}^d(V, F)) = 0$. (If you have time, think about what happens when $d < n$.)

[1] "Anyone who is going to do any work with lattices needs to understand Smith invariants." – John Stembridge

(d) Show that $\dim(\mathrm{Alt}^n(V, F)) \leq 1$

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 3a (Due September 28)

(76) Let $q(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$.
  (a) Show that $q(x)$ is irreducible in $\mathbb{Z}[x]$.
  (b) Suppose p is a prime. Show that if a and b are nonsquares in $(\mathbb{Z}/(p))^\times$, then ab is a square in $(\mathbb{Z}/(p))^\times$. Conclude that the image of at least one of 2, 3, and 6 is a square in $(\mathbb{Z}/(p))^\times$. [You can do this problem without knowing that $(\mathbb{Z}/(p))^\times$ is cyclic, so don't assume this in your solution.]
  (c) Suppose p is a prime. Let $\bar{q}$ denote the image of q in $(\mathbb{Z}/(p))[x]$.
    (i) If the image of 2 in $(\mathbb{Z}/(p))^\times$ is a square, factor $\bar{q}$ in $(\mathbb{Z}/(p))[x]$. [Hint: $q(x) = (x^2-1)^2 - 8x^2$.]
    (ii) If the image of 3 in $(\mathbb{Z}/(p))^\times$ is a square, factor $\bar{q}$ in $(\mathbb{Z}/(p))[x]$. [Hint: $q(x) = (x^2+1)^2 - 12x^2$.]
    (iii) If the image of 6 in $(\mathbb{Z}/(p))^\times$ is a square, factor $\bar{q}$ in $(\mathbb{Z}/(p))[x]$. [Hint: $q(x) = (x^2-5)^2 - 24$.]
  (d) Conclude that q is irreducible, yet reducible modulo every prime.

(77) Let R be an integral domain with field of fractions F and let $q(x)$ be a monic polynomial in $R[x]$. Assume that $q = ab$ where $a, b \in F[x]$ are monic polynomials of smaller degree than q. Prove that if $a \notin R[x]$, then R is not a UFD. Conclude (again!) that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD. [Your proof should not be more than ten short lines.]

(78) Suppose that R is a commutative ring, $D \subset R$ is multiplicative, and $I \subset R \setminus D$ is an ideal.
  (a) Show that there exists an ideal $J \subset R$ that is maximal with respect to the properties:
    - $I \subset J$
    - $J \cap D = \emptyset$.
  (b) Suppose $\mathfrak{m} \subset R$ is an ideal that is maximal with respect to the properties $I \subset \mathfrak{m}$ and $\mathfrak{m} \cap D = \emptyset$. Show that $\mathfrak{m}$ is a prime ideal.

(79) Suppose R is a ring and $\varphi \in \mathrm{Hom}(R,R) = \mathrm{Hom}_{\mathrm{ring}}(R,R)$. For all $n \in \mathbb{N}$ define $\varphi^n = \varphi \circ \varphi \circ \cdots \circ \varphi \in \mathrm{Hom}(R,R)$.
  (a) Show that if φ is surjective, then φ^n is surjective.
  (b) Let $I_n = \ker(\varphi^n)$. Show that I_n is an ideal and $I_1 \subset I_2 \subset I_3 \subset \cdots$.
  (c) Suppose R is Noetherian. Show that if φ is surjective, then φ is injective.
  (d) Is the converse of Homework 79c true?

(80) Let $R = \mathbb{Z}[\sqrt{-5}]$ and $M = (2, 1-\sqrt{-5}) \subset R$. Define $f \in \mathrm{Hom}_R(R^2, M)$ by $f([x,y]^T) = x2 + y(1+\sqrt{-5})$. Find $\vec{a}, \vec{b} \in R^2$ so that $\vec{x} \in \ker(f)$ if and only if $\vec{x} \in R\vec{a} + R\vec{b}$. [We say that $(\vec{a}, \vec{b})$ is a list of *generators* for $\ker(f)$.]

(81) Repeat Homework 70a, but with $\mathbb{Z}$ replaced by Euclidean Domain, R. [1]

(82) EROs and ECOs: Smith Normal Form over a Euclidean Domain, R. Suppose that A is a nonzero $n \times m$ matrix with entries in R.
  (a) Let b_{11} be the nonzero g.c.d. of all entries in A. Show[2] that there are elementary matrices $E_1', E_2', \ldots, E_r'$ and $F_1', F_2', \ldots, F_c'$ with entries in R so that $C = E_r' \cdot E_{r-1}' \cdots E_2' \cdot E_1' \cdot B \cdot F_1' \cdot F_2' \cdots F_{c-1}' \cdot F_c'$ has the form

$$\begin{pmatrix} b_{11} & 0 & 0 & \cdots & 0 \\ 0 & c_{22} & c_{23} & \cdots & c_{2m} \\ 0 & c_{32} & c_{33} & \cdots & c_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

  where b_{11} divides c_{ij} for all $2 \le i \le n$ and $2 \le j \le m$.

---

[1] Hint: WOLOG, $A \neq 0$. Let $N\colon R \to \mathbb{Z}_{\ge 0}$ be a norm on R (as in [DF04, p. 270]). Transform A into the form $\begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix}$ with $N(b_{11}) \le N(b_{22})$. If $b_{11} \nmid b_{22}$, then transform the above matrix into the form $\begin{pmatrix} b_{11} & b_{22}' \\ 0 & b_{22} \end{pmatrix}$ where $b_{11} = db_{22} + b_{22}'$ and $N(b_{22}') < b_{11}$ ....

[2] Hint: Since $A \neq 0$, we may define $\delta(A) := \min\{N(a_{ij}) \mid a_{ij} \neq 0\}$. Via EROs and ECOs we may assume that $N(a_{11}) = \delta(A)$. If $a_{k1} \neq 0$, write $a_{k1} = a_{11}z_k + z_{k1}$ where $0 < N(z_{k1}) < N(a_{11})$. Via EROs, we may replace a_{k1} with z_{k1}, and we have a new matrix, Z, for which $\delta(Z) < \delta(A)$. Via EROs and ECOs we may assume $N(z_{11}) = \delta(Z)$. Since the image of N is a bounded below discrete set, continuing in this fashion (and also repeating the above procedure for the first row), we arrive at a matrix Z where the only nonzero entry in the first row and first column is z_{11}. Of course, it will almost certainly be the case that z_{11} does not divide each z_{ij}. Suppose $z_{11} \nmid z_{ij}$. Look at the two-by-two submatrix $\begin{pmatrix} z_{11} & 0 \\ 0 & z_{ij} \end{pmatrix}$ and mimic Homework 81. Since the image of N is a bounded below discrete set, continuing in this fashion we arrive at a matrix C where the only nonzero entry in the first row and first column is c_{11} and $c_{11} \mid c_{ij}$ for all i and j.

(b) Apply induction to conclude that via EROs and ECOs applied to A we can arrive at a matrix

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

where D is a diagonal (square) matrix with nonzero entries $a_1, a_2, \ldots, a_k$ satisfying $k \leq \min\{m, n\}$ and $a_1 \mid a_2 \mid \cdots \mid a_k$. This is called the Smith Normal Form of A. As we shall see later, it is unique (up to units).

(c) Let $R = \mathbb{Q}[x]$. Compute the Smith Normal Form of

$$\begin{pmatrix} x-2 & 0 \\ 0 & x-5 \end{pmatrix} \text{ and } \begin{pmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{pmatrix}.$$

(For extra uniqueness: we require all nonzero polynomials that occur in the Smith Normal Form be monic.)

(d) If F is a field, then what is the Smith Normal Form of $A \in \mathrm{Mat}_{n\times m}(F)$?

(83) Suppose R is a rng (yes, rng, not ring). Let I be an ideal of R. Show that the correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrngs A of R that contain I and the set of subrngs of R/I. Show that a subrng C of R that contains I is an ideal in R if and only if C/I is an ideal in R/I. What if we replace "rng" with "ring" in the above? [Hint: look at pretty much any non-prime ideal in $\mathbb{Z}$.]

(84) A characterization of PIDs. Suppose R is a nonzero commutative ring. Prove that R is a PID if and only if R is a UFD for which the Bezout Property[1] holds (see Homework 66). [Hint: One direction is immediate. For the other direction: suppose I is an ideal with two generators. Since R is a UFD, each element of I may be written as a product of irreducible factors. Choose $a \in I$ to have a minimal number of irreducible factors. Prove that $I = (a)$ by showing that if there is a $b \in I \setminus (a)$, then $(a, b) = (d)$ leads to a contradiction.]

(85) Suppose k is a field, V is a vector space of one dimension over k, and $T \in \mathrm{Hom}_k(V, V)$. Show that, as $k[x]$-modules, V is isomorphic to $k[x]/(x-\mu)$ for some $\mu \in k$. How unique is μ? Are they isomorphic as $k[x]$-algebras?

(86) Suppose A is a $\mathbb{Z}$-module. Recall that for $m \in \mathbb{N}$ we set ${}_mA = \{a \in A \mid ma = 0\}$.

(a) Show that if $m = rs$ and $(r, s) = 1$, then ${}_mA = {}_rA + {}_sA$.

(b) Conclude that if we write m as $m = \prod_{p|m} p^{e(p)}$ with p prime and $e(p) \in \mathbb{N}$, then ${}_mA = \sum_{p|m} {}_{p^{e(p)}}A$.

Definition. Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories. A *functor* or *covariant functor* from $\mathcal{C}$ to $\mathcal{D}$ is a mapping that

- assigns to every object $C \in \mathcal{C}$ an object $F(C) \in \mathcal{D}$ and
- assigns to every morphism $f\colon C \to C'$ in $\mathcal{C}$ a morphism $F(f)\colon F(C) \to F(C')$ in $\mathcal{D}$

such that $F(\mathrm{Id}_C) = \mathrm{Id}_{F(C)}$ for every object $C \in \mathcal{C}$ and $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f\colon C \to C'$ and $g\colon C' \to C''$.

(87) Show that the map P from the category Set to itself that sends a set X to the powerset of X and sends a morphism $f\colon X \to Y$ in Set to to $P(f)\colon P(X) \to P(Y)$ where

$$P(f)(U) = f[U] := \{f(x) \mid x \in U\}$$

is a functor.

Definition. Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories. A *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$ is a mapping that

- assigns to every object $C \in \mathcal{C}$ an object $F(C) \in \mathcal{D}$ and
- assigns to every morphism $f\colon C \to C'$ in $\mathcal{C}$ a morphism $F(f)\colon F(C') \to F(C)$ in $\mathcal{D}$

such that $F(\mathrm{Id}_C) = \mathrm{Id}_{F(C)}$ for every object $C \in \mathcal{C}$ and $F(g \circ f) = F(f) \circ F(g)$ for all morphisms $f\colon C \to C'$ and $g\colon C' \to C''$.

(88) (*) Show that the map Q from the category Set to itself that sends a set X to the powerset of X and sends a morphism $f\colon X \to Y$ in Set to to $Q(f)\colon Q(Y) \to Q(X)$ where

$$Q(f)(V) = f^{-1}[V] := \{x \in X \mid f(x) \in V\}$$

is a contravariant functor.

[1] Every ideal generated by two elements is a principal ideal.

(89) Suppose k is a field and Vec_k is the category of finite dimensional k-vector spaces. Show that the map D from Vec_k to itself which assigns to each vector space its dual space and to every linear map its dual map is a contravariant functor.

(90) (*) Suppose that R is a UFD. Show that $R[x_1, x_2, \ldots, x_m]$ is a UFD.

Math 593. Homework 3b (Due October 1)

(91) Suppose k is a field and V and W are finite dimensional k-vector spaces with bases $\mathbf{v}$ and $\mathbf{w}$, respectively. The choice of bases gives us a bijective map $T \mapsto {}_{\mathbf{w}}[T]_{\mathbf{v}}$ between $\mathrm{Hom}_k(V, W)$ and $\mathrm{Mat}_{\dim(W)\times\dim(V)}(k)$. Thus, a linear map between an n-dimensional k-vector space and an m-dimensional k-vector space can be encoded in a natural way by nm numbers. Suppose U is a third k-vector space with basis $\mathbf{u}$.
  (a) Can you think of a way to encode a k-bilinear map from $V \times W$ to U?
  (b) Suppose $f \in \mathrm{Bil}_k(V \times W, U)$. Let $((v_i, w_i) \colon 1 \leq i \leq n)$ be a list of vectors in $V \times W$. When is f completely determined by the values $f(v_i, w_i)$? I will be happy if you can come up with good answers for the cases when $V = W = U$ and $\dim(V) \in \{1, 2\}$.

(92) Determinant problem
  (a) Show that $\det \in \mathrm{Alt}^n(F^n, F)$, so $\dim(\mathrm{Alt}^n(F^n, F)) = 1$. (Recall that $\det(v_1, v_2, v_3, \ldots, v_n)$ with $v_i \in F^n$ is the determinant of the $n \times n$ matrix whose columns are v_1 through v_n.)
  (b) Suppose V is an n-dimensional F-vector space and let $\mathbf{v}$ be a basis for V. Define $f \colon V \times V \times \cdots \times V \to F$ by $f(x_1, x_2, \ldots, x_n) = \det([x_1]_{\mathbf{v}}, [x_2]_{\mathbf{v}}, \ldots, [x_n]_{\mathbf{v}})$. Show $f \in \mathrm{Alt}^n(V, F)$ and conclude that $\dim(\mathrm{Alt}^n(V, F)) = 1$.
  (c) Continuing the notation of (92b). Suppose that $T \in \mathrm{End}(V)$ and $h \in \mathrm{Alt}^n(V, F)$ is nonzero. (*i*) Show that the function $h_T \colon V \times V \times \cdots \times V \to F$ defined by $h_T(x_1, x_2, \ldots, x_n) = h(T(x_1), T(x_2), \ldots, T(x_n))$ belongs to $\mathrm{Alt}^n(V, F)$. (*ii*) Conclude that there is a constant $d \in F$ for which $h_T = dh$. (*iii*) Show that this constant is independent of the choice of nonzero h.
  (d) Thanks to the previous problem, we can define $\det(T)$ to be the unique element of F for which $h_T = \det(T)h$ for any nonzero $h \in \mathrm{Alt}^n(V, F)$. Show: if $S, T \in \mathrm{End}(V)$, then $\det(S \circ T) = \det(S)\det(T)$.
  (e) Show that if $T \in \mathrm{End}(V)$ is invertible, then $\det(T) \neq 0$.
  (f) Suppose that $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ are two bases of V that are related by the change of coordinate matrix $A = {}_{\mathbf{u}}[\mathrm{Id}_V]_{\mathbf{w}}$. Show that for any $g \in \mathrm{Alt}^n(V, F)$ we have $g(w_1, w_2, \ldots, w_n) = \det(A)g(u_1, u_2, \ldots, u_n)$.
  (g) Show that if $T \in \mathrm{End}(V)$ has nonzero determinant, then T is invertible.

Something to Think About

In Homework 84 you showed that a UFD is a PID if and only if the Bezout property holds. It is also true that a UFD is a PID if and only if every nonzero prime ideal is maximal. Can you show this?

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 4a (Due October 5)

(93) Does $(8x + 7x^4, 4x^2 + 19x^4, x^2)$ generate the ideal $I = (x^3, 4x^2, 8x)$ in $\mathbb{Z}[x]$?

(94) Suppose R is a ring. Let I and J be ideals of R with $I \subset J$. Show that J/I is an ideal of R/I and $(R/I)/(J/I)$ is isomorphic to R/J as rings. Describe $(\mathbb{Z}/24\mathbb{Z})/(6\mathbb{Z}/24\mathbb{Z})$.

(95) Suppose k is a field.
- (a) Suppose V is a k-vector space and $T \in \mathrm{End}_k(V)$. Show that V is a $k[x]$-module where $pv = p(T)v$ for $p \in k[x]$ and $v \in V$.
- (b) Show that if M is a $k[x]$-module, then M is a k-vector space and there exists $T \in \mathrm{End}_k(V)$ so that for $p \in k[x]$ and $v \in V$ we have $pv = p(T)v$.
- (c) Conclude that modules over $k[x]$ are parameterized by pairs (V, T) where V is a k-vector space and $T \in \mathrm{End}_k(V)$.

(96) Suppose that R is a commutative ring.
- (a) Suppose $\mathfrak{p} \subset R$ is a prime ideal and $x \in R$ is nilpotent. Show that $x \in \mathfrak{p}$.
- (b) Suppose $y \in R$ and $y \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Show that y is nilpotent. [Hint: Homework 78 may be useful.]
- (c) Conclude that $x \in R$ is nilpotent if and only if x belongs to every prime ideal in R. That is

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}.$$

(97) Let R be a ring and M a free module over R. Let I be a set, and let $(m_i \mid i \in I)$ be a basis of M. Let N be an R-module, and let $(n_i \mid i \in I)$ be a family of elements of N.
- (a) Show that there is a unique $f \in \mathrm{Hom}_R(M, N)$ such that $f(m_i) = n_i$ for all $i \in I$.
- (b) Show that if $(n_i \mid i \in I)$ is a linearly independent spanning set for N, then f is an isomorphism.

(98) Suppose that R is a commutative ring. Suppose $I \subset R$ is an ideal and M is an R-module.
- (a) Show that IM is a submodule of M and M/IM is an R/I module.
- (b) Show that if M is a finitely generated R-module, then M/IM is a finitely generated R/I-module. Is the converse true?
- (c) Show that for all $n \in \mathbb{Z}_{\geq 0}$ we have that $I^n M/I^{n+1}M$ is an R/I module.

(99) Suppose that R is a commutative ring.
- (a) Suppose $I \subset R$ is an ideal and M is a free R-module with basis $(s_i \mid i \in I)$. Show that M/IM is a R/I free module and M/IM has basis $(\bar{s}_i \mid i \in I)$ where $\bar{s}_i$ denotes the image of s_i in the R/I- module Rs_i/Is_i
- (b) Suppose that J and K are sets. Show that $R^{\oplus K}$ is isomorphic to $R^{\oplus J}$ if and only if $K \simeq J$ as sets. [Hint, quotient out by a maximal ideal.] This result is false if R is not commutative – see [DF04, Exercise 27 in §10.3]. Does this failure in the noncommutative case contradict Exercise 97b?

Thanks to Prompt (123) and Homework (99), the following definition makes sense.

Definition. Suppose R is a commutative ring and M is a free R-module. The *rank* of the free R-module M is defined to be the cardinality of I where $M \simeq \bigoplus_{i \in I} R$.

(100) Show that any nonzero principal ideal in a domain R has free rank one.

(101) Suppose K is a field.
- (a) Suppose $f \in k[x]$. Is $k[x]/(f)$ a cyclic k-module? If not, can you formulate some conditions on f which will guarantee that $k[x]/(f)$ is cyclic?
- (b) Suppose V is a k-vector space and $T \in \mathrm{Hom}_k(V, V)$. Is V a cyclic $k[T]$ module for every nonzero $v \in V$? Is V always a cyclic $k[x]$-module? If not, can you formulate some conditions on T which will ensure V is a cyclic $k[T]$-module?

(102) Let $R = \{p \in \mathbb{Q}[x] \colon p(0) \in \mathbb{Z}\}$. Show that R is a ring. Let $I = \{p \in R \colon p(0) = 0\}$. Is I a finitely generated R-module?

(103) Beyond EROs and ECOs: Smith Normal Form over a PID, R. Suppose that A is a nonzero $n \times m$ matrix with entries in R. Since R is a PID, it is a UFD. Thus every nonzero element $a \in R$ can be written as a unit times $\ell(a)$ primes. So, for example, $\ell(p^3) = 3$ where p is a prime and $\ell(u) = 0$ when $u \in R^\times$. We call $\ell(a)$ the length of a; it will play the role of N in the footnote to Homework (82). Define $\delta(A) = \min\{\ell(a_{ij}) \mid a_{ij} \neq 0\}$.
- (a) We begin with the case of a 2×2 nonzero matrix A with entries in R. After elementary operations, we may assume that $\ell(a_{11}) = \delta(A)$. If $a_{11} \mid a_{12}$, then perform ECOs to make the $(1, 2)$ entry zero. Otherwise,

suppose $a_{11} \nmid a_{12}$. Thanks to Homework 84, if $d = \gcd(a_{11}, a_{12})$, then we can find $\alpha, \beta \in R$ for which $\alpha a_{11} + \beta a_{12} = d$. Right multiply A by the invertible (why is it invertible?) matrix

$$G = \begin{pmatrix} \alpha & a_{12}/d \\ \beta & -a_{11}/d \end{pmatrix}.$$

Magic! Note that $\ell(d) < \ell(a_{11})$, so $\delta(AG) < \delta(A)$. Now do something similar to the first column. We arrive at a diagonal matrix C for which $\delta(C) \leq \delta(A)$. If $c_{11} \mid c_{22}$, we are done. Otherwise ...

(b) Now suppose A is an $n \times m$ matrix with entries in R. Show that there exist an invertibe $n \times n$ matrix Q and an invertible $m \times m$ matrix P so that

$$QAP = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

where D is a diagonal (square) matrix with nonzero entries $a_1, a_2, \ldots, a_k$ satisfying $k \leq \min\{m, n\}$ and $a_1 \mid a_2 \mid \cdots \mid a_k$. This is called the Smith Normal Form of A. As we shall see later, it is unique (up to units).

(104) Suppose R is a ring and M is a finitely generated R-module. Must submodules of M also be finitely generated? [Hint: Let $M = R = \mathbb{R}[x_1, x_2, \ldots]$. Consider $N = (x_1, x_2, \ldots)$.]

(105) Suppose A is a $\mathbb{Z}$-module and $p \in \mathbb{N}$ is prime. Let $A(p)$ denote those $x \in A$ for which some power of p annihilates x. That is, $A(p) = \bigcup_{m \in \mathbb{N}} A_{p^m}$. (Here we use the notation of Homework 86.)

(a) Is $A(p)$ a subgroup of A?

(b) Describe $(\mathbb{Q}/\mathbb{Z})(p)$.

(c) If p and q are distinct primes in $\mathbb{N}$, what is $A(p) \cap A(q)$?

(106) Suppose R is a ring and L, M, N, and P are R-modules. Suppose

$$0 \to M \to N \to P \to 0$$

is an exact sequence of R-modules.

(a) (covariant) Show that the mapping from the category of R-modules to the category of abelian groups given by $X \mapsto \mathrm{Hom}_R(L, X)$ and $\alpha \in \mathrm{Hom}_R(X, Y)$ maps to $\alpha_* \colon \mathrm{Hom}_R(L, X) \to \mathrm{Hom}_R(L, Y)$ where $\alpha_*(f) = \alpha \circ f$ is a functor. Then show it is a *left exact functor*; that is:

$$0 \to \mathrm{Hom}_R(L, M) \to \mathrm{Hom}_R(L, N) \to \mathrm{Hom}_R(L, P)$$

is an exact sequence of abelian groups.

(b) (contravariant) Show that the mapping from the category of R-modules to the cateogry of abelian groups given by $X \mapsto \mathrm{Hom}_R(X, L)$ and $\alpha \in \mathrm{Hom}_R(X, Y)$ maps to $\alpha^* \colon \mathrm{Hom}_R(Y, L) \to \mathrm{Hom}_R X, L)$ where $\alpha^*(f) = f \circ \alpha$ is a contravariant functor. Then show it is a *left exact contravariant functor*; that is:

$$0 \to \mathrm{Hom}_R(P, L) \to \mathrm{Hom}_R(N, L) \to \mathrm{Hom}_R(M, L)$$

is an exact sequence of abelian groups.

(107) Suppose R is a commutative ring and L, M, and F are R-modules. Show that if F is a free module of finite rank, then the short exact sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} F \longrightarrow 0$$

splits; that is there is an R-module isomorphism $\varphi \colon M \simeq L \oplus F$ for which the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{Id}_F} & & \\ 0 & \longrightarrow & L & \xrightarrow{\iota} & L \oplus F & \xrightarrow{\pi} & F & \longrightarrow & 0 \end{array}$$

where ι is the natural injection and π is the natural projection. *Bonus.* Show that the condition that F be finite rank is not needed. *Bonus 2.* Do we need to assume that R is commutative?

Math 593. Homework 4b (Due October 8)

(108) Suppose F is a field, V is a finite-dimensional F-vector space, and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is a basis of V. Show that the map $\mathrm{End}_k(V) \to \mathrm{Mat}_{n \times n}(k)$ given by $T \mapsto_{\mathbf{v}} [T]_{\mathbf{v}}$ is a k-algebra isomorphism.

(109) Recall that if A is an $n \times n$ matrix with entries in a field F, then $\mathrm{tr}(A) = \sum_{i=1}^n A_{ii}$.

(a) Show that for all $n \times n$ matrices we have $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. Conclude that

(i) if C is invertible, then $\mathrm{tr}(A) = \mathrm{tr}(CAC^{-1})$, and
(ii) if C is nilpotent, then $\mathrm{tr}(C) = 0$.

(b) Suppose V is a finite dimensional F-vector space and $T \in \mathrm{Hom}_F(V, V)$. Show that $\mathrm{tr}({}_{\mathbf{v}}[T]_{\mathbf{v}})$ is independent of the choice of the basis $\mathbf{v}$. We define $\mathrm{tr}(T) = \mathrm{tr}({}_{\mathbf{v}}[T]_{\mathbf{v}})$.

(c) Suppose V and V' are finite dimensional F-vector spaces. Choose $T \in \mathrm{Hom}_F(V, V')$ and $T' \in \mathrm{Hom}_F(V', V)$. Show that $\mathrm{tr}(T \circ T') = \mathrm{tr}(T' \circ T)$.

Something to Think About

Suppose R is a ring. Must every short exact sequence of R-modules of the form

$$0 \longrightarrow L \longrightarrow L \oplus N \longrightarrow N \longrightarrow 0$$

split?

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 5a (Due October 12)

(110) (*) Suppose R is a domain, M is a torsion free R-module, and $r \in R$. Show that $\mu_r \in \mathrm{Hom}_R(M, M)$ defined by $\mu_r(m) = rm$ is injective.

(111) How many abelian groups have both of the following properties:
  (a) any minimal generating set has 3 elements
  (b) the exponent[1] is 30.

(112) Suppose R is an integral domain and M is a finitely generated R-module. Prove that M is a torsion module if and only if $\mathrm{Ann}_R(M) \neq \{0\}$.

(113) Suppose A is an $n \times n$ matrix. Do A and A^T have the same
  (a) minimal polynomial?
  (b) characteristic polynomial?
  (c) rational canonical form?

(114) Just as for rings (see Homework 59), there are many equivalent ways to think about Noetherian modules. Show the following are equivalent for an R-module M.
  (a) M is Noetherian.
  (b) Every non-empty set S of submodules of M has a maximal element.
  (c) Every submodule of M is finitely-generated.

(115) Suppose R is a ring, M is an R-module, and $\varphi \in \mathrm{Hom}_R(M, M)$. For all $n \in \mathbb{N}$ define $\varphi^n = \varphi \circ \varphi \circ \cdots \circ \varphi \in \mathrm{Hom}_R(M, M)$.
  (a) Show that if φ is surjective, then φ^n is surjective.
  (b) Let $M_n = \ker(\varphi^n)$. Show that M_n is a submodule and $M_1 \subset M_2 \subset M_3 \subset \cdots$.
  (c) Suppose M is Noetherian. Show that if φ is surjective, then φ is injective.
  (d) *Bonus.* From Homework 79c we know the converse to Homework 115c is false. However, if M satisfies the descending chain condition (that is, M is Artinian[2]), then an injective map $\varphi\colon M \to M$ is surjective. Prove it.

Homework (14), Homework (44), and Homework (115) are variations on a very useful theme. You will probably encounter many similar statements in your study of mathematics; my favorite such statement is the Ax-Grothendieck[3] theorem[4]: if $f\colon \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then f is surjective. Moreover, $f^{-1}\colon \mathbb{C}^n \to \mathbb{C}^n$ is also a polynomial map.

(116) Show that the invariant factor form of the Structure Theorem for Finitely Generated Modules over a PID together with the Chinese Remainder Theorem implies the elementary divisor form of the structure theorem. [Hint: Use Prompt 59.]

(117) Let R be a PID and suppose A is an $n \times m$ matrix with entries in R. For $1 \leq k \leq \max(n, m)$, a $k \times k$ *minor* of A is the determinant of a $k \times k$ matrix obtained from A by deleting $n - k$ rows and $m - k$ columns. Let $I_k(A)$ denote the ideal of R generated by the $k \times k$ minors of A. So, for example, for the matrix

$$B = \begin{pmatrix} 3 & 4 & 12 \\ 8 & 6 & 18 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$$

we have $I_1(B) = \mathbb{Z}$ and $I_2(B) = (14)$. Suppose $n, m \in \mathbb{N}$ and $1 \leq k \leq \max(n, m)$.
  (a) Show that if $X \in \mathrm{Mat}_{n\times m}(R)$, then $I_k(X) = I_k(X^T)$.
  (b) Show that if $C \in \mathrm{Mat}_{n\times m}(R)$ and $D \in \mathrm{Mat}_{m\times m}(R)$, then $I_k(CD) \subset I_k(C)$.

[Hint: write $C = \begin{bmatrix} | & | & & | \\ C_1 & C_2 & \cdots & C_m \\ | & | & & | \end{bmatrix}$, so $CD = \begin{bmatrix} | & | & & | \\ \sum_{i=1}^m D_{i1}C_i & \sum_{i=1}^m D_{i2}C_i & \cdots & \sum_{i=1}^m D_{im}C_i \\ | & | & & | \end{bmatrix}$.]

  (c) Show that if $Q \in \mathrm{Mat}_{n\times n}(R)^\times$, $A \in \mathrm{Mat}_{n\times m}(R)$, and $P \in \mathrm{Mat}_{m\times m}(R)^\times$, then $I_k(A) = I_k(QAP)$.

---

[1] The *exponent* of a group is defined to be the least common multiple of the orders of all elements of the group.

[2] Named for Emil Artin. His family changed their surname from Artinian to Artin, otherwise we would have Artinianian rings. Also, every Artinian ring is Noetherian: C. Hopkins, *Rings with minimal condition for left ideals*, Annals of Mathematics (2), vol. 40 (1939) no. 2, 712-730.

[3] James Ax and Alexander Grothendiek are well worth reading about.

[4] This is an easy-to-state consequence of the result; the full result is about varieties over algebraically closed fields.

(d) Suppose $A, A' \in \mathrm{Mat}_{n\times m}(R)$. We say that A and A' are equivalent[1] matrices provided that $A' = QAP$ for some $Q \in \mathrm{Mat}_{n\times n}(R)^\times$ and $P \in \mathrm{Mat}_{m\times m}(R)^\times$. Show that every equivalence class of matrices has a unique (up to units in R) element that is in Smith Normal Form.

(118) Suppose A is a $\mathbb{Z}$-module. Recall that for a prime p we define the submodule $A(p) = \bigcup_{m\in\mathbb{N}} A_{p^m}$ where $A_{p^m} = \{a \in A \,|\, p^m a = 0\}$.

(a) Suppose $p_1, p_2, \ldots, p_n$ are distinct primes and $x_i \in A(p_i)$. Show that if $\sum x_i = 0$, then $x_1 = x_2 = \cdots = x_n = 0$.

(b) Show that the natural map $\bigoplus_p A(p) \to A$ is injective.

(c) Conclude that if A is a torsion group, then

$$\bigoplus_p A(p) \simeq A.$$

[Hint: Homeworks 86b and 68c may be useful.]

(119) Suppose R is a Noetherian integral domain. Let M be a finitely generated R-module and suppose $\varphi \in \mathrm{Hom}_R(R^{\oplus n}, M)$ is surjective. Show that $\ker(\varphi)$ is finitely generated.

(120) Suppose k is a field and V is a k-vector space. Suppose $S, T \in \mathrm{Hom}_k(V, V)$. Show that if the corresponding $k[x]$-modules are isomorphic, then S is similar to T. The converse is true as well, see Prompt 184.

(121) Suppose R is a PID and F is a finitely generated free R-module. Suppose $M \subset F$ is a submodule. Show M is free. [Hint: You are **not** allowed to use the Structure Theorem for Finitely Generated Modules over a PID. Suppose $F \simeq R^k$. Proceed by induction on k and use Prompt 129c and Homework 107.] (*Bonus.*) Show that the result is true without the assumption that F is finitely generated.

Definition. Suppose R is a ring, M is an R-module, and $m \in M$. The *annihilator of* m is

$$\mathrm{Ann}_R(m) := \{r \in R \,|\, rm = 0\}.$$

If no confusion is possible, we will write $\mathrm{Ann}(m)$ rather than $\mathrm{Ann}_R(m)$.

(122) Suppose R is a commutative ring, M is an R-module, and $I \subset R$ is an ideal. Show that M contains a copy of R/I if and only if $I = \mathrm{Ann}(m)$ for some $m \in M$.

(123) Suppose R is a commutative ring and

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is a short-exact sequence of R-modules. Suppose $N \simeq \oplus N_j$ where each N_j is a cyclic R-module (i.e., $N_j = Rn_j$ for some $n_j \in N_j$). Show: If there exists $m_j \in M$ such that

- $\beta(m_j) = n_j$ and
- $\mathrm{Ann}_R(m_j) = \mathrm{Ann}_R(n_j)$,

then $M \simeq L \oplus N$. [It is mathematical shorthand to write $\beta(m_2) = n_2$ when we really mean $\phi \circ \beta(m_2) = (0, n_2, 0, \ldots)$ where $\phi\colon N \simeq \oplus N_j$. Also, Homework 122 may be useful.]

(124) Suppose R is a PID, M is a finitely generated R-module, and $(p) \subset R$ is a prime ideal. Define

$$M(p) = \{m \in M \,|\, p^n m = 0 \text{ for some } n \in \mathbb{Z}_{\geq 0}\}.$$

(Why is $M(p)$ well defined?) Show that if $m \in M(p)$ then there exists $k \in \mathbb{Z}_{\geq 0}$ for which $\mathrm{Ann}_R(m) = (p^k)$.

(125) (*Bonus.*) Suppose R is a commutative ring and M is an R-module. Set $\mathcal{I} = \{\mathrm{Ann}(m) \,|\, m \in M \setminus \{0\}\}$. Show that a maximal element of $\mathcal{I}$ is a prime ideal of R. [This is the start of an important circle of ideas in commutative algebra; see, for example, the Lasker-Noether theorem.]

[1] Check that this is an equivalence relation!

Please report any errors you find to smdbackr@umich.edu

Definition. Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories and F is a functor from $\mathcal{C}$ to $\mathcal{D}$. For every pair of objects $C, C' \in \mathcal{C}$ the functor F defines a function

$$F_{C,C'}: \ \mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C), F(C')).$$

The functor F is said to be *faithful* if $F_{C,C'}$ is injective for every pair of objects $C, C' \in \mathcal{C}$. The functor F is said to be *full* if $F_{C,C'}$ is surjective for every pair of objects $C, C' \in \mathcal{C}$. A functor that is both faithful and full is said to be *fully faithful*. The functor F is said to be *essentially surjective* provided that each object D of $\mathcal{D}$ is isomorphic to $F(C)$ for some object C of $\mathcal{C}$. We say that $\mathcal{C}$ and $\mathcal{D}$ are *equivalent* if there is a fully faithful essentially surjective functor from $\mathcal{C}$ to $\mathcal{D}$.

(126) Suppose k is a field. Let $\mathcal{D}$ denote the category of $k[x]$-modules. Let $\mathcal{C}$ be as in Homework 31. Extend the result of Homework 95 to show that $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

Math 593. Homework 5b (Due October 15)

Fall Break – nothing due.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 6a (Due October 17)
(That's a Wednesday!)

Fall Break and Exam – light homework

(127) Suppose R is a PID. Let M be a finitely generated R-module and suppose $f \in \mathrm{Hom}_R(R^\ell, M)$ is surjective. Thanks to Homework (119), we know $\ker(f)$ is finitely generated. Thus, we can find a finite generating set $\mathbf{y} = (y_1, y_2, \ldots, y_t)$ for $\ker(f)$. Suppose $\mathbf{x} = (x_1, x_2, \ldots, x_\ell)$ is a basis for R^ℓ. Write

$$y_j = \sum_i a_{ij} x_i$$

for some $a_{ij} \in R$. The matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1t} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{\ell 1} & a_{\ell 2} & a_{\ell 3} & \cdots & a_{\ell t} \end{pmatrix}$$

is called a *presentation matrix*. [The transpose of A is often called a *relations matrix*.]

(a) Show $A(R^t) = \ker(f)$; conclude that $M \simeq R^\ell / A(R^t)$.
(b) Show that for all invertible $P \in \mathrm{Mat}_{t\times t}(R)$ we have $AP(R^t) = \ker(f)$.
(c) Show that for all invertible $Q \in \mathrm{Mat}_{\ell\times\ell}(R)$ we have $M \simeq R^\ell/A(R^t) \simeq R^\ell/(QA(R^t))$.
(d) Show that for all invertible $Q \in \mathrm{Mat}_{\ell\times\ell}(R)$ and all invertible $P \in \mathrm{Mat}_{t\times t}(R)$ we have $M \simeq R^\ell/(QAP(R^t))$.
(e) Let

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & & \end{pmatrix} \text{ with } a_1 \mid a_2 \mid \cdots \mid a_k$$

be a Smith Normal Form of A. Use your work above and Homework 117 to conclude that

$$M \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^{\ell-k}.$$

What does Homework (117d) tell us about the uniqueness of this decomposition? [Note, if a_j is a unit in R, then $R/(a_j)$ is zero.]

(128) The Cayley-Hamilton Theorem is a very powerful tool. For example, if R is a commutative ring, then the commutative ring version of the Cayley-Hamilton Theorem can be used to prove that every surjective R-linear map from a finitely generated R-module to itself is, in fact, an isomorphism (compare to Homework 115). Here we look at matrix exponentiation and related constructions. Suppose $f\colon \mathbb{C} \to \mathbb{C}$ is an analytic function (like, for example, sin or exp). Let V be a finite dimensional $\mathbb{C}$-vector space, and fix $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$. Let $p \in \mathbb{C}[x]$ denote the characteristic polynomial of T.

(a) Show that we can write $f = pq + r$ where $0 \le \deg(r) < \deg(p)$. What sort of function is q?
(b) Show that $f(T) = r(T)$ and for every eigenvalue λ of T we have $f(\lambda) = r(\lambda)$.
(c) Write $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r^{n-1}x^{n-1}$. Suppose T has n-distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. We have n equations $r(\lambda_i) = f(\lambda_i)$ in the n unknowns $r_0, r_1, r_2, \ldots, r_{n-1}$. Show that we can always solve for the r_j, hence we have

$$f(T) = \sum_{j=0}^{n-1} r_j T^j$$

for *known* coefficients $r_j \in \mathbb{C}$.
(d) Find e^{At} and $\sin(At)$ for

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} -1 & -4 \\ 5 & 0 \end{bmatrix}, \text{ and } \quad A = \begin{bmatrix} -8 & -18 & 6 \\ 8 & 18 & -5 \\ 4 & 12 & -1 \end{bmatrix}.$$

(e) (*Bonus.*) Suppose the eigenvalues of T are not distinct. Let μ be an eigenvalue of T that occurs with multipliciy $m > 1$. Note that p and its first $(m-1)$ derivatives are zero at μ. Show we have

$$f^{(j)}(\mu) = r^{(j)}(\mu)$$

where $0 \leq j \leq (m-1)$. Conclude that we can still solve for the coefficients of r.

(129) Suppose that k is a field, V is finite dimensional k-vector space, and $T \in \mathrm{Hom}_k(V,V)$. We assume that $\chi_T(x)$ factors completely into linear factors. Let $\lambda_1, \lambda_2, \ldots, \lambda_m$ be the distinct eigenvalues for T, so $\chi_T(x) = \prod_{i=1}^m (x-\lambda_i)^{n_i}$. **Warning**: $(x-\lambda_i)^{n_i}$ is not, in general, an invariant factor for T.

(a) Show that $V_i = \ker(T-\lambda_i)^{n_i}$ is T stable and $V = \oplus_{j=1}^m V_j$.

(b) Show that there exists $f \in k[x]$ such that $f(x) \in (x)$ and $f(x) \equiv \lambda_i \mod (x-\lambda_i)^{n_i}$ for $1 \leq i \leq m$.

(c) Set $g(x) = x - f(x)$. Let $T_s = f(T)$ and $T_n = g(T)$. Show that $T = T_s + T_n$, T_n is nilpotent, T_s is semisimple, and $T_n \circ T_s = T_s \circ T_n$.

(d) Show that if $T = S + N$ where S is semisimple, N is nilpotent, and $S \circ N = N \circ S$, then $S = T_s$ and $N = T_n$.

Math 593. Homework 6b (Due October 22)

(130) Suppose F is a field and V, W are F-vector spaces.

(a) Suppose V has dimension greater than zero. Suppose $S \subset V$ is a list of vectors. Show that S is a basis of V if and only if every nonzero vector in V can be written in a unique way as a linear combination of vectors in S with nonzero coefficients.

(b) Suppose B is a basis for V and $f\colon B \to W$ is a function. There is a unique $T \in \mathrm{Hom}_F(V,W)$ such that $T(b) = f(b)$ for all $b \in B$.

(c) Suppose B is a basis for V and $T, S \in \mathrm{Hom}_F(V,W)$. If $T(b) = S(b)$ for all $b \in B$, then $T = S$.

(d) If V is a finite dimensional F-vector space of dimension n, then V is isomorphic to F^n.

(131) Adjoints and all that. Suppose F is a field and V, W are finite dimensional F-vector spaces. Recall that $V^* = \mathrm{Hom}_F(V,F)$ is called the dual space of V. For $T \in \mathrm{Hom}_F(V,W)$ define $T^* \in \mathrm{Hom}_F(W^*, V^*)$ by setting $T^*(\lambda) = \lambda \circ T$ for $\lambda \in W^*$. The linear map T^* is called the *adjoint* of T.

(a) Let $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be a basis for V. For $1 \leq j \leq n$ show there is a unique $\lambda_j \in V^*$ satisfying $\lambda_j(v_i) = \delta_{ij}$. Show that the list $\mathbf{v}^* = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ is a basis for V^*. [It is called the *dual basis* of V; note that its definition relies on the choice of $\mathbf{v}$.]

(b) If $T \in \mathrm{Hom}_F(V,W)$, then ${}_{\mathbf{v}^*}[T^*]_{\mathbf{w}^*} = {}_{\mathbf{w}}[T]^t_{\mathbf{v}}$.

(c) Suppose that $T \in \mathrm{End}_F(V) := \mathrm{Hom}_F(V,V)$. Show that $\det(T) = \det(T^*)$.

(d) Suppose V and W are finite dimensional real vector spaces equipped with inner products $\langle , \rangle_V$ and $\langle , \rangle_W$ respectively. Show that the map $v \mapsto \langle -, v\rangle_V$ identifies V with V^* and, similarly, $w \mapsto \langle -, w\rangle_W$ identifies W with W^*.

(e) Recall that under the identifications introduced in problem (131d) we have that T^* becomes the unique map from W to V which satisfies $\langle w, T(v)\rangle_W = \langle T^*(w), v\rangle_V$ for all $v \in V$ and $w \in W$. Under what conditions on $\mathbf{v}$ and $\mathbf{w}$ is it true that ${}_{\mathbf{v}}[T^*]_{\mathbf{w}} = {}_{\mathbf{w}}[T]^t_{\mathbf{v}}$? [Hint: Many students have serious difficulties with this problem.]

(f) An element $T \in \mathrm{End}(V)$ is called *self-adjoint* provided that under the identification introduced in problem (131e) we have $T = T^*$. If T is self-adjoint, then what can we say about ${}_{\mathbf{v}}[T]_{\mathbf{v}}$?

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 7a (Due October 26)

(132) Use the Structure Theorem for Modules over a PID together with Homework 10 to show that if F is a finite field, then $F^\times$ is a cyclic group.

(133) Suppose R is a commutative ring and M is an R-module. Show that the following are equivalent.
- M is finitely presented.
- There is a short exact sequence
$$0 \to K \to F \to M \to 0$$
where F is a free R-module and both K and F are finitely generated R-modules.
- There is an exact sequence
$$F' \to F \to M \to 0,$$
where both F' and F are finitely generated free R-modules.

(134) Suppose R is a commutative ring and $I \subset R$ is an ideal. Show that if I is a free R-module, then I is a principal ideal. Under what conditions on R does the converse hold?

(135) Suppose R is a commutative ring. Let I, J be ideals in R. Show that there is an exact sequence of R-modules
$$0 \longrightarrow I \cap J \longrightarrow R \xrightarrow{\beta} R/I \times R/J \longrightarrow R/(I+J) \longrightarrow 0$$
where $\beta(r) = (r + I, r + J)$. How is this related to the Chinese Remainder Theorem?

(136) (*) Suppose R is a commutative ring. When is $\{0\}$ a prime ideal in R?

(137) Suppose R is a ring and M is an R-module. If N, P are submodules of M, then
- $N + P$ is a submodule of M,
- $N \cap P$ is a submodule of M, and
- $(N + P)/N \simeq P/(N \cap P)$.

(Compare to Homework 63.)

(138) Suppose k is a field and V is a finite dimensional k-vector space. Fix $B \in \mathrm{Bil}(V \times V, k)$.
(a) Define $L_B \colon V \to V^*$ by $L_B(v)(v') = B(v, v')$. Show $L_B \in \mathrm{Hom}_k(V, V^*)$.
(b) Define $R_B \colon V \to V^*$ by $R_B(v)(v') = B(v', v)$. Show $R_B \in \mathrm{Hom}_k(V, V^*)$.
(c) Show that under the natural identification of V^{**} with V we have $L_B^* = R_B$ and $R_B^* = L_B$.
(d) Conclude that L_B and R_B have the same rank. (Recall that for k-vector spaces U, W and $T \in \mathrm{Hom}_k(U, W)$ the *rank* of T is the dimension of $\mathrm{im}(T)$.)

(139) Suppose R is a ring and M is an R-module. If N, P are submodules of M with $N \leq P$, then $(M/N)/(P/N) \simeq M/P$. (Compare to Homework 94.)

(140) Suppose R is a ring, M and N are R-modules, and $f \in \mathrm{Hom}_R(M, N)$ is surjective. Show that $M/\ker(f) \simeq N$.

(141) Suppose k is a field, $M \in \mathrm{Mat}_{n\times n}(k)$ with $M = -M^T$, and $Q \in \mathrm{Mat}_{n\times n}(k)^\times$. Show that if all of the diagonal entries of M are zero, then the same is true for $Q^T M Q$. What if we don't assume that Q is invertible? [*Nota Bene*. If the characteristic of k is not two, then $M = -M^T$ implies that the diagonal entries of M are all zero.]

(142) Suppose k is a field and V, W are finite dimensional k-vector spaces. Show that $V \otimes_k W^* \simeq \mathrm{Hom}_k(W, V)$.

(143) EROs and ECOs: Suppose k is a field. A matrix $A \in \mathrm{Mat}_{n\times n}$ is *symmetric* provided that $A = A^T$.
(a) Suppose $n = 2$ and $A \in \mathrm{Mat}_{2\times 2}$ is symmetric. Show that if the characteristic of k is not two, then we can find $Q \in \mathrm{Mat}_{2\times 2}(k)^\times$ for which $Q^T A Q$ is diagonal.
(b) Let $A \in \mathrm{Mat}_{n\times n}$ be symmetric. Show that if the characteristic of k is not two, then we can find $Q \in \mathrm{Mat}_{n\times n}(k)^\times$ for which $Q^T A Q$ is diagonal.
(c) Show that there is a $Q \in \mathrm{Mat}_{2\times 2}(\mathbb{Q})^\times$ so that
$$Q^T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} Q = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$
(d) Show that if the characteristic of k is two, then for $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ the matrix $Q^T A Q$ is not diagonal for all $Q \in \mathrm{Mat}_{2\times 2}(k)^\times$.

(144) Suppose R is a ring and
$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is a short exact sequence of R-modules. Show that if there exists $f \in \mathrm{Hom}_R(N, M)$ for which $\beta \circ f = \mathrm{Id}_N$, then the sequence splits; that is, there is an isomorphism $\varphi\colon M \simeq L \oplus N$ for which the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{Id}_N} & & \\ 0 & \longrightarrow & L & \xrightarrow{\iota} & L \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

where ι is the natural injection and π is the natural surjection.

(145) Suppose R is a ring. Consider the following commutative diagram consisting of two (horizontal) exact sequences of R-modules linked by (vertical) R-module homomorphisms.

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & & \end{array}$$

(a) Show that we have well-defined maps $\bar{\alpha}\colon \mathrm{coker}(f) \to \mathrm{coker}(g)$ and $\bar{\beta}\colon \mathrm{coker}(g) \to \mathrm{coker}(h)$.

(b) Show that the sequence

$$\mathrm{coker}(f) \xrightarrow{\bar{\alpha}} \mathrm{coker}(g) \xrightarrow{\bar{\beta}} \mathrm{coker}(h)$$

is exact.

(c) Show that if β is surjective, then $\bar{\beta}$ is surjective.

Math 593. Homework 7b (Due October 29)

(146) Choosing wisely. In physics one typically develops theories that are coordinate-free. However, when it comes time to actually solve a problem, one must choose an appropriate coordinate system. The story is similar in linear algebra; and eigenvalues and eigenvectors sometimes give us a way to choose coordinates wisely (and thus use change of coordinate matrices, etc.). Recall that the Fibonacci sequence begins $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$. The nth Fibonacci number, F_n, is given by the rules: $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

(a) Define the linear transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ by $T(\vec{e}_1) = \vec{e}_1 + \vec{e}_2$ and $T(\vec{e}_2) = \vec{e}_1$ where $(\vec{e}_1, \vec{e}_2)$ is the standard basis for $\mathbb{R}^2$. Is T injective? surjective? invertible?

(b) Let $A = {}_{\mathbf{e}}[T]_{\mathbf{e}}$ be the matrix that represents T with respect to the standard basis $\mathbf{e} = (\vec{e}_1, \vec{e}_2)$. Show that for $m \geq 1$ we have

$$\begin{bmatrix} F_{m+1} \\ F_m \end{bmatrix}_{\mathbf{e}} = A \begin{bmatrix} F_m \\ F_{m-1} \end{bmatrix}_{\mathbf{e}} = A^m \begin{bmatrix} 1 \\ 0 \end{bmatrix}_{\mathbf{e}}.$$

(c) Thus, to compute the 43th Fibonacci number, we need only compute A^{42}. Convince yourself that this is a bit unreasonable to compute. ("He chose poorly.")

(d) It would be awesome if we could find linearly independent vectors $\vec{v}_1, \vec{v}_2 \in \mathbb{R}^2$ and distinct $\lambda_1, \lambda_2 \in \mathbb{R}$ such that $T(\vec{v}_i) = \lambda_i \vec{v}_i$. Supposing this is possible, write down the matrix $B = {}_{\mathbf{v}}[T]_{\mathbf{v}}$ that represents T with respect to the basis $\mathbf{v} = (\vec{v}_1, \vec{v}_2)$. Can you compute B^{43}? Supposing $\vec{v}_1$ and $\vec{v}_2$ exist, how unique will they be?

(e) How to compute these $\vec{v}_1, \vec{v}_2 \in \mathbb{R}^2$ and $\lambda_1, \lambda_2 \in \mathbb{R}$? Show that if Id denotes the identity map on $\mathbb{R}^2$, then $\vec{v}_i$ is in the kernel of the linear transformation $(T - \lambda_i \,\mathrm{Id})$.

(f) We know that a linear transformation from $\mathbb{R}^2$ to $\mathbb{R}^2$ has a nontrivial kernel if and only if the determinant of the associated matrix with respect to $\vec{e}_1$ and $\vec{e}_2$ is zero. Compute this determinant for $(T - \lambda_i \,\mathrm{Id})$ to find the values of λ_1 and λ_2.

(g) Now, how do we find $\vec{v}_1$ and $\vec{v}_2$? That's right, we compute the kernel of $(T - \lambda_i \,\mathrm{Id})$. Thankfully, we know how to do this via Gauss-Jordan, so do it. If possible, normalize your vectors so that $[\vec{v}_i]_{\mathbf{e}}$ has a one in its second entry. (That is, write $\vec{v}_i$ as $??\vec{e}_1 + \vec{e}_2$).

(h) Write down $B = {}_{\mathbf{v}}[T]_{\mathbf{v}}$, the matrix that represents T with respect to the basis $\mathbf{v} = (\vec{v}_1, \vec{v}_2)$. (Hint: This is meant to be easy, I just want you to remember what you are doing!)

(i) Recall how to move between the (ordered) basis $\mathbf{e} = (\vec{e}_1, \vec{e}_2)$ and the (ordered) basis $\mathbf{v} = (\vec{v}_1, \vec{v}_2)$. (Wait, how do we know that $(\vec{v}_1, \vec{v}_2)$ is a basis for $\mathbb{R}^2$?). Thankfully, this is pretty straightforward – we just need to compute ${}_{\mathbf{v}}[\mathrm{Id}]_{\mathbf{e}}$ to move from the choice of coordinate system $\mathbf{e}$ to the choice of coordinate system $\mathbf{v}$. Similarly, we compute ${}_{\mathbf{e}}[\mathrm{Id}]_{\mathbf{v}}$ to move from $\mathbf{v}$ to $\mathbf{e}$. Compute $M = {}_{\mathbf{v}}[\mathrm{Id}]_{\mathbf{e}}$ and $N = {}_{\mathbf{e}}[\mathrm{Id}]_{\mathbf{v}}$. Show that $NM = MN = \mathrm{Id}_2$ (Hint:

$$\mathrm{Id}_2 = {}_{\mathbf{e}}[\mathrm{Id}]_{\mathbf{e}} = {}_{\mathbf{v}}[\mathrm{Id}]_{\mathbf{v}} = {}_{\mathbf{v}}[\mathrm{Id} \circ \mathrm{Id}]_{\mathbf{v}} = {}_{\mathbf{v}}[\mathrm{Id}]_{\mathbf{e}}\ {}_{\mathbf{e}}[\mathrm{Id}]_{\mathbf{v}} \quad \text{etc.})$$

(j) Using $T = \mathrm{Id} \circ T \circ \mathrm{Id}$, show $A^m = M^{-1}B^m M$.

(k) Compute the mth Fibonacci number.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 8a (Due November 2)

(147) Suppose that k is a field not of characteristic two. Suppose that V is a k-vector space.
  (a) Show that there is an involution $f \in \mathrm{Hom}_k(V \otimes_k V, V \otimes_k V)$ for which $f(v_1 \otimes v_2) = v_2 \otimes v_1$ for all $v_1, v_2 \in V$.
  (b) Show that the eigenvalues of f are ± 1. [Note: we are not assuming finite dimensionality, so you cannot use determinants.]
  (c) Show that $V \otimes_k V = (V \otimes_k V)(1) \oplus (V \otimes_k V)(-1)$. If V is finite dimensional, what are the dimensions of $(V \otimes_k V)(1)$ and $(V \otimes_k V)(-1)$?
  (d) How is this related to Prompt 294?

(148) If it makes sense, describe each of the following tensor products.
  (a) $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C}$, $\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{C}$, $\mathbb{R}^n \otimes_{\mathbb{C}} \mathbb{C}$, and $\mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}$.
  (b) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$. Does this suggest anything?

(149) Suppose R is a commutative ring and M, N are unital R-modules. Show that $\sum_{i=1}^n m_i \otimes n_i = \sum_{j=1}^\ell m'_j \otimes n'_j$ in $M \otimes_R N$ if and only if $\sum_{i=1}^n \varphi(m_i, n_i) = \sum_{j=1}^\ell \varphi(m'_j, n'_j)$ for all bilinear $\varphi\colon M \times N \to P$.

(150) Suppose R is a commutative ring. If M is an R-module and F is a free R-module with basis $(f_i\colon i \in I)$, then every element of $M \otimes_R F$ has a unique representation as $\sum_{i \in I} m_i \otimes f_i$ with abfm $m_i = 0$. [Hint: You may want to use Prompt (228a).]

(151) Suppose $a, b \in \mathbb{Z}_{>1}$ and $d = (a, b)$.
  (a) Show that the map $\varphi\colon \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ given by $\varphi(x, y) = xy \mod d$ is $\mathbb{Z}$-bilinear.
  (b) Show that $\bar{\varphi}\colon \mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ is surjective. [Hint: What is $\bar{\varphi}(1 \otimes y)$?]
  (c) Show that $|\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z}| \leq d$. [Hint: 1 spans $\mathbb{Z}/a\mathbb{Z}$ and 1 spans $\mathbb{Z}/b\mathbb{Z}$, so $1 \otimes 1$ spans $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z}$ (why?). Show that the order of $1 \otimes 1$ divides d.]
  (d) Conclude that $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$.

(152) (a) Suppose R is a commutative ring and M, N, and P are unital R-modules. Suppose $f \in \mathrm{Hom}(M \otimes_R N, P)$. Does there exist a bilinear map $B\colon M \times N \to P$ such that $B(m, n) = f(m \otimes n)$ for every $(m, n) \in M \times N$? If so, how unique is B?
  (b) Show that $\mathrm{Bil}_R(M \times N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$.
  (c) (Tensor-hom adjunction) Show that $\mathrm{Hom}_R(M \otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$.
  (d) Conclude that $(M \otimes_R N)^* \simeq \mathrm{Hom}_R(M, N^*)$.

(153) Here is a different (and important for base change) version of Homework 152c. Suppose R, S are commutative rings. Suppose $f \in \mathrm{Hom}(R, S)$. We can think of an S-module B as an R module by setting $r \cdot b = f(r)b$ for $b \in B$ and $r \in R$. Suppose P is an R-module and M is an S-module. We have:

$$\mathrm{Hom}_S(M, \mathrm{Hom}_R(S, P)) \simeq \mathrm{Hom}_R(M \otimes_S S, P) \simeq \mathrm{Hom}_R(M, P)$$

as abelian groups. To say it in a more sophisticated way:

$$\mathrm{Hom}_S(\cdot, \mathrm{Hom}_R(S, P)) \simeq \mathrm{Hom}_R(\cdot \otimes_S S, P) \simeq \mathrm{Hom}_R(\cdot, P)$$

as functors from the category of S-modules to the category of abelian groups. (Note: for $\mu \in \mathrm{Hom}_R(S, P)$ and $s', s \in S$ we have $(s' \cdot \mu)(s) = \mu(s's)$.) [Hint: Suppose $\alpha \in \mathrm{Hom}_S(M, \mathrm{Hom}_R(S, P))$. Define $\varphi\colon M \times S \to P$ by $\varphi(m, s) = (\alpha(m)(s))$. Note that $\alpha(m) \in \mathrm{Hom}_R(S, P)$, so $(\alpha(m)((f(r)s) = r((\alpha(m))(s))$.]

(154) Suppose R is a commutative ring, I is an ideal in R, and M is an R-module.
  (a) Show that $R/I \otimes_R M \simeq M/IM$. How unique is this isomorphism?
  (b) Conclude that $R \otimes_R M \simeq M$.
  (c) Describe $a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/bZ$.
  (d) Suppose P is an R module. Is there a bijective correspondence between the set of bilinear maps from $R \times M$ to P and $\mathrm{Hom}_R(M, P)$?

(155) Suppose k is a field and V and W are finite dimensional k-vector spaces.
  (a) Show that the following chain of linear isomorphisms holds.

$$\mathrm{Hom}_k(V, W) \simeq W \otimes_k V^* \simeq W^{**} \otimes_k V^* \simeq V^* \otimes_k W^{**} \simeq \mathrm{Hom}_k(W^*, V^*).$$

  Verify that the isomorphism from left to right is the familiar one that sends $T \in \mathrm{Hom}_k(V, W)$ to $T^* \in \mathrm{Hom}_k(W^*, V^*)$ where $T^*(\lambda) = \lambda \circ T$ for all $\lambda \in W^*$.
  (b) Show that

$$V^* \otimes_k W^* \simeq (V \otimes_k W)^*.$$

[Hint: If $\lambda \otimes \mu \in V^* \otimes_k W^*$, then we have a map $(v \otimes w \mapsto \lambda(v)\mu(w)) \dots$]

(c) Show that the following chain of linear isomorphisms holds.

$$\mathrm{Hom}_k(V,W)^* \simeq (W \otimes_k V^*)^* \simeq W^* \otimes_k V^{**} \simeq W^* \otimes_k V \simeq V \otimes_k W^* \simeq \mathrm{Hom}_k(W,V).$$

Note that this chain identifies $\mathrm{Hom}_k(W,V)$ and $\mathrm{Hom}_k(V,W)$ as dual to each other, hence it produces a nondegenerate pairing

$$\tau\colon\ \mathrm{Hom}_k(W,V) \times \mathrm{Hom}_k(V,W) \to k.$$

Show that $\tau(T,S) = \mathrm{tr}(T \circ S) = \mathrm{tr}(S \circ T)$.

(156) Suppose R is a ring. Consider the following commutative diagram consisting of two (horizontal) exact sequences of R-modules linked by (vertical) R-module homomorphisms.

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & & \end{array}$$

(a) Show that the sequence

$$\ker(f) \longrightarrow \ker(g) \longrightarrow \ker(h)$$

makes sense and is exact.

(b) Show that if α' is injective, then the map from $\ker(f)$ to $\ker(g)$ is also injective.

(157) Suppose R is a ring and

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is a short exact sequence of R-modules. Show that if there exists $g \in \mathrm{Hom}(M,L)$ for which $g \circ \alpha = \mathrm{Id}_L$, then the sequence splits; that is, there is an isomorphism $\varphi\colon M \simeq L \oplus N$ for which the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{Id}_N} & & \\ 0 & \longrightarrow & L & \xrightarrow{\iota} & L \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

where ι is the natural inclusion and π is the natural surjection. Compare to Homework 144.

Suppose R is ring and $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is an exact sequence of R-modules. If B is another R-module, then for every $f \in \mathrm{Hom}_R(B,L)$ there is a (unique) map $\tilde{f} \in \mathrm{Hom}_R(B,M)$ so that the following diagram commutes

$$\begin{array}{ccccccccc} & & & & B & & & & \\ & & & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \tilde{f}} & & & \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

Indeed, this is basically the proof that $X \mapsto \mathrm{Hom}_R(B,X)$ is left exact. (See Homework 106.) (Un)fortunately, the same thing is not true if instead of looking at maps from B to L, we look at maps from L to B. That is, if $g \in \mathrm{Hom}_R(L,B)$, then there need not exist $\bowtie \in \mathrm{Hom}_R(M,B)$ that makes the following diagram commute.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \bowtie} & & & & & \\ & & B & & & & & & \end{array}$$

(158) Show that if R is a field, then for all $g \in \mathrm{Hom}_R(L,B)$ there exists $\bowtie \in \mathrm{Hom}_R(M,B)$ so that the above diagram commutes.

(159) Show by example that the map $\bowtie$ need not exist in the category of $\mathbb{Z}$-modules. [Hint: Take $L = M = B = \mathbb{Z}$.]

Definition. Suppose R is a ring. An R-module Q is said to be *injective* provided that for every exact sequence $0 \longrightarrow L \longrightarrow M$ of R-modules and for every $g \in \mathrm{Hom}_R(L, Q)$ there exists $\tilde{g} \in \mathrm{Hom}_R(M, Q)$ so that the following diagram commutes

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & M \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \tilde{g}} & \\ & & Q & & \end{array}$$

(160) Show that R cannot, in general, be injective in the category of R-modules. [Suppose $r \in R$ is a non-zero-divisor and consider the map $\mu_r \in \mathrm{Hom}_R(R, R)$ given by $\mu_r(s) = rs$. Look at $0 \longrightarrow R \xrightarrow{\mu_r} R \longrightarrow R/(r) \longrightarrow 0$. Take $Q = R$ and $g = \mathrm{Id}_R$.]

Homework 160 shows that if Q is to be injective, then for all ideals I of R and all maps $g \in \mathrm{Hom}_R(I, Q)$, we need to find a map $\tilde{g} \in \mathrm{Hom}_R(R, Q)$ extending g (that is, $\mathrm{res}_I \tilde{g} = g$). This suggests that we need something like: for all non-zero-divisors $r \in R$ we need $rQ = Q$. In the category of $\mathbb{Z}$-modules, we know of two such modules:

(161) Show that $\mathbb{Q}$ and/or $\mathbb{Q}/\mathbb{Z}$ are injective in the category of $\mathbb{Z}$-modules. [Hint: Suppose $L \leq M$ are $\mathbb{Z}$-modules and $g \in \mathrm{Hom}_R(L, \mathbb{Q})$. Consider the set

$$\mathcal{S} = \{(g', M') \mid L \leq M' \leq M \text{ and } \mathrm{res}_L\, g' = g\}.$$

For $(g', M'), (g'', M'') \in \mathcal{S}$ we write $(g', M') \leq (g'', M'')$ provided that $M' \leq M''$ and $\mathrm{res}_{M'}\, g'' = g'$. Show that Zorn's Lemma applies ...]

We will have more to say about injective modules later.

Math 593. Homework 8b (Due November 5)

(162) Suppose k is a field and V is a k-vector space. Suppose $v, v' \in V$. Under what conditions do we have $v \otimes v' = v' \otimes v$ in $V \otimes_k V$?

(163) Suppose that $(V, \langle\ ,\ \rangle)$ is a finite dimensional real inner product space. Suppose $T \in \mathrm{Hom}(V, V)$. Show that the following are equivalent:

(a) T preserves distances i.e., $\|T(v) - T(w)\| = \|v - w\|$ for all $v, w \in V$.
(b) $\langle T(v), T(w)\rangle = \langle v, w\rangle$ for all $v, w \in V$. (We say T preserves the inner product.)
(c) $T^* \circ T = T \circ T^* = \mathrm{Id}_V$.
(d) T maps any orthonormal basis of V to an orthonormal basis of V.
(e) For any orthonormal basis $\mathbf{v}$ of V, the columns of ${}_{\mathbf{v}}[T]_{\mathbf{v}}$ form an orthonormal basis of $\mathbb{R}^n$ with respect to the standard inner product on $\mathbb{R}^n$.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 9a (Due November 9)

(164) Suppose k is a field and $A, B \in \mathrm{Mat}_{n\times n}(k)$. We say that A is *cogredient* to B provided that there is a $Q \in \mathrm{Mat}_{n\times n}(k)^\times$ for which $Q^T AQ = B$.
  (a) Show that cogredient matrices have the same rank.
  (b) Suppose A and B are cogredient. Show that $\det(A) \neq 0$ if and only if $\det(B) \neq 0$.

(165) Suppose k is a field and $R = k[x, y]/(xy)$. Let $M = R/(x)$ and $N = R/(y)$.
  (a) Show that $\lambda\colon M \to R$ which maps $m \in M$ to the image of ym in R belongs to M^*. Show that the map $m \mapsto \dot{m}\lambda$, where $\dot{m} \in R$ is any representative for m, induces a well-defined isomorphism $T\colon M \to M^*$.
  (b) Show that $M \otimes_R N = R/(x, y) \simeq k$.
  (c) Conclude that $M^* \otimes_R N^* \simeq M \otimes_R N \simeq k$.
  (d) Use tensor-hom adjunction to show $(M \otimes_R N)^* = 0$. Compare to Exercise 155b.
  (e) *Remark/Problem*. Exercise 155b can fail to generalize for many reasons – here is another example that shows why finitely generated is needed: Suppose R is a commutative ring and let P be a (unital) free module with R-basis $(p_n)_{n\in\mathbb{N}}$. Define $B\colon P \times P \to R$ by $B(p_n, p_m) = \delta_{m,n}$. Let $\mu \in (P \otimes_R P)^*$ be the (unique) corresponding linear map. Show that μ is not in the image of the natural map $P^* \otimes_R P^* \to (P \otimes_R P)^*$.

(166) Suppose k is a field and V, W are finite dimensional k-vector spaces. Suppose $\varphi \in \mathrm{Hom}_k(V, V)$ and $\tau \in \mathrm{Hom}_k(W, W)$.
  (a) Show $\mathrm{tr}(\varphi \otimes \tau) = \mathrm{tr}(\varphi)\,\mathrm{tr}(\tau)$.
  (b) Show $\det(\varphi \otimes \tau) = \det(\varphi)^{\dim(W)} \det(\tau)^{\dim(V)}$. [HINT: $\varphi \otimes \tau = (\mathrm{Id}_V \otimes \tau) \circ (\varphi \otimes \mathrm{Id}_W)$.]

(167) Suppose R is a ring. Show that if M, M', N, and N' are finitely generated free R-modules, then the map $S\colon \mathrm{Hom}_R(M, M') \otimes_R \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$ of Prompt (239) is an isomorphism.

(168) Put $A = \mathbb{C} \otimes_R \mathbb{C}$. Since $\mathbb{C}$ is an $\mathbb{R}$-algebra, thanks to Prompt (279) (c.f. [DF04, Proposition 21]), we know that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$-algebra where $(\sum a_i \otimes b_i)(\sum c_k \otimes d_k) = \sum_{i,k}(a_i c_k \otimes b_i d_k)$. Let (b_1, b_2, b_3, b_4) be the $\mathbb{R}$-basis of A given by $b_1 = 1 \otimes 1$, $b_2 = 1 \otimes i$, $b_3 = i \otimes 1$, and $b_4 = i \otimes i$.
  (a) Show that $(b_4 - 1_A)(b_4 + 1_A) = 0$, so A is not an integral domain. [What is the identity of the ring A?]
  (b) Show that as an $\mathbb{R}$-module, the left ($r\cdot\sum z_i\otimes w_i = \sum rz_i\otimes w_i$) and right actions ($(\sum z_i\otimes w_i)\cdot r = \sum z_i\otimes rw_i$) of $\mathbb{R}$ on A are the same. However, as a $\mathbb{C}$-module (via extension of scalars), the left and right actions of $\mathbb{C}$ on A are not the same.
  (c) Let $e_1 = 1/2(b_1 + b_4)$ and $e_2 = 1/2(b_1 - b_4)$. Show that $e_1e_2 = e_2e_1 = 0$, $e_1 + e_2 = 1_A$, $e_1^2 = e_1$ and $e_2^2 = e_2$. Conclude that $A \simeq Ae_1 \times Ae_2$. [Hint: Exercise 28 may be useful.]
  (d) Prove that the map $\varphi\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ that sends (z, w) to $(zw, z\bar{w})$ is an $\mathbb{R}$-bilinear map.
  (e) Let $\Phi\colon A \to \mathbb{C} \times \mathbb{C}$ denote the unique $\mathbb{R}$-linear map obtained from φ. Show that $\Phi(e_1) = (0, 1)$ and $\Phi(e_2) = (1, 0)$. Show that Φ is $\mathbb{C}$-linear where the action on A is the left action and the action on $\mathbb{C} \times \mathbb{C}$ is given by $z(w_1, w_2) = (zw_1, zw_2)$. Deduce that Φ is surjective, and hence defines a $\mathbb{C}$-algebra isomorphism of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ with $\mathbb{C} \times \mathbb{C}$.

(169) Suppose k is a field. Does a short exact sequence of vector spaces always split?

Suppose R is ring and $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is an exact sequence of R-modules. If A is another R-module, then for every $f \in \mathrm{Hom}_R(A, L)$ there is a (unique) map $\tilde{f} \in \mathrm{Hom}_R(A, M)$ so that the following diagram commutes

$$\begin{array}{ccccccccc} & & & & A & & & & \\ & & & & \downarrow f & \searrow^{\tilde{f}} & & & \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

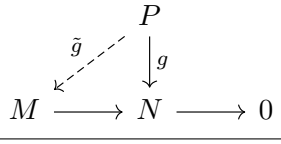
Indeed, this is basically the proof that $X \mapsto \mathrm{Hom}_R(A, X)$ is left exact. (See Homework 106.) (Un)fortunately, the same thing is not true at the right-hand of the sequence. That is, if $g \in \mathrm{Hom}_R(A, N)$, then there need not exist a projection ☺ from A to M that makes the following diagram commute.

$$\begin{array}{ccccccccc} & & & & & & A & & \\ & & & & & \swarrow_{\text{☺}} & \downarrow g & & \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

(170) Show by example that the map ☺ need not exist.

(171) Show that if A is free, then the map ☺ must exist. [Hint: Choose a basis.]

Definition. Suppose R is a ring. An R-module P is said to be *projective* provided that for every exact sequence $M \longrightarrow N \longrightarrow 0$ of R-modules and for every $g \in \mathrm{Hom}_R(P, N)$ there exists $\tilde{g} \in \mathrm{Hom}_R(P, M)$ so that the following diagram commutes



(172) Show that every free R-module is projective.

(173) Show that $\mathbb{Z}/2\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module. [Hint: Use the Chinese Remainder Theorem.] Is $\mathbb{Z}/2\mathbb{Z}$ a free $\mathbb{Z}/6\mathbb{Z}$-module?

Toward the end of term, projective and injective modules will help us study the failure of exactness for various functors.

(174) Suppose R is ring.
- (a) Show that an R-module is projective if and only if the functor $X \mapsto \mathrm{Hom}_R(P, X)$ is exact.
- (b) Show that an R-module is injective if and only if the functor $X \mapsto \mathrm{Hom}_R(X, Q)$ is exact.

(175) Suppose R and S are commutative rings and let Q be an injective R module. Suppose $f \in \mathrm{Hom}(R, S)$. Show that $f^!(Q) = \mathrm{Hom}_R(S, Q)$ is an injective S-module. ($s \in S$ acts on $\alpha \in \mathrm{Hom}_R(S, Q)$ by $(s\alpha)(s') = \alpha(ss')$, and for $r \in R$ we have $\alpha(f(r)s') = r(\alpha(s'))$.) [Hint: Use tensor-hom adjunction (see Homework 153).]

(176) Suppose R is a commutative ring. Show that the category of R-modules admits non-trivial injective modules. [Hint: You may wish to use Prompt 4, Homework 161, and Homework 175.]

Math 593. Homework 9b (Due November 12)

(177) Suppose that $(V, \langle\,,\,\rangle)$ is a finite dimensional real inner product space. A linear transformation $T \in \mathrm{Hom}(V, V)$ satisfying any of the equivalent conditions in (163) is said to be an *orthogonal transformation* of V with respect to $\langle\,,\,\rangle$. Let $\mathrm{O}(V, \langle\,,\,\rangle)$ denote the set of orthogonal transformations on V. People usually write $\mathrm{O}(V)$ rather than $\mathrm{O}(V, \langle\,,\,\rangle)$ if there is no possibility for confusion.
- (a) Show that $T \in \mathrm{O}(V)$ if and only if $T^* \in \mathrm{O}(V)$. Conclude that T is an orthogonal transformation if and only if for any orthonormal basis $\mathbf{v}$ of V, the rows of ${}_{\mathbf{v}}[T]_{\mathbf{v}}$ form an orthonormal basis of $\mathbb{R}^n$ with respect to the standard inner product on $\mathbb{R}^n$.
- (b) Show that if $g \in \mathrm{O}(V)$, then $\det(g) \in \{\pm 1\}$.
- (c) Show that if $a, b \in \mathrm{O}(V)$, then $ab = a \circ b \in \mathrm{O}(V)$. That is, composition defines a binary operation on $\mathrm{O}(V)$.
- (d) Show that $\mathrm{O}(V)$ is a group; it is called the orthogonal group (for $(V, \langle\,,\,\rangle)$). That is, show: (a) the binary operation on $\mathrm{O}(V)$ is associative; (b) there is an identity element $e \in \mathrm{O}(V)$ such that $ea = ae = a$ for all $a \in \mathrm{O}(V)$; and (c) for every $x \in \mathrm{O}(V)$ there is an inverse $y \in \mathrm{O}(V)$ such that $xy = yx = e$. [Note: we have already proved that if e exists, it is unique. We have also proved that when inverses exist, they are unique. You should review the proofs of those statements – do you need associativity?]
- (e) We set $\mathrm{SO}(V) = \mathrm{SO}(V, \langle\,,\,\rangle) = \{h \in \mathrm{O}(V, \langle\,,\,\rangle) \mid \det(h) = 1\}$. $\mathrm{SO}(V)$ is called the special orthogonal group (for $(V, \langle\,,\,\rangle)$). Show that $\mathrm{SO}(V)$ is a subgroup of $\mathrm{O}(V)$. That is, $\mathrm{SO}(V)$ is a group and it is a subset of $\mathrm{O}(V)$. Show also that $\mathrm{SO}(V)$ is a normal subgroup of $\mathrm{O}(V)$, that is: for all $g \in \mathrm{O}(V)$ and $h \in \mathrm{SO}(V)$ we have $ghg^{-1} \in \mathrm{SO}(V)$.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 10a (Due November 16)

(178) Suppose $p \in \mathbb{Z}$ is a prime number.
  (a) Show that $p\mathbb{Z} \simeq \mathbb{Z}$ as $\mathbb{Z}$-modules.
  (b) What is $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$?
  (c) What is $p\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$?
  (d) Look at the inclusion $\iota\colon p\mathbb{Z} \to \mathbb{Z}$ and consider the image of $p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ under $\iota \otimes \mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}}$. What is it?

(179) Suppose A is an abelian group. What is $A \otimes_{\mathbb{Z}} \mathbb{Z}$?

(180) Suppose k is a field. Suppose $A \in \mathrm{Mat}_{n\times n}(k)$ and set $B_A(x,y) = x^T(Ay)$.
  (a) Show that $B_A \in \mathrm{Bil}(k^n \times k^n, k)$.
  (b) Show that B_A is symmetric if and only if A is *symmetric* (that is, $A = A^T$).
  (c) Show that B_A is alternating if and only if A is *skew-symmetric* (that is $A = -A^T$) and the diagonal entries of A are zero.
  (d) Show that B_A is skew-symmetric if and only if A is *skew-symmetric*.

(181) Show: If M is a finitely generated R-module, then $\mathrm{Alt}^d_R(M,P) = 0$ for all $d >> 0$. What can you say about $\mathrm{Sym}^d_R(M,P)$?

Suppose k is $\mathbb{R}$ or $\mathbb{C}$ and V is a k-vector space of dimension n. In physics, a (contravariant) tensor of rank ℓ is a quantity with ℓ indices, e.g. $A^{\mu_1\mu_2\cdots\mu_\ell}$, whose Cartesian components $\tilde{A}^{\mu_1\mu_2\cdots\mu_\ell}$ in a new coordinate system are obtained from the original ones by the rule

$$\tilde{A}^{\mu_1\mu_2\cdots\mu_\ell} = \sum_{1\le\nu_1,\nu_2,\ldots,\mu_\ell\le n} A^{\nu_1\nu_2\cdots\mu_\ell} a_{\mu_1\nu_1} a_{\mu_2\nu_2} \cdots a_{\mu_\ell\nu_\ell}$$

where $(a_{\mu\nu})$ is the matrix expressing the first coordinate system of V in terms of the second.

(182) If the notation in this problem is correct, it is a miracle. Suppose k is $\mathbb{R}$ or $\mathbb{C}$ and let V denote an n-dimensinal k-vector space. Let $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ be a basis for V. An element $T \in V^{\otimes\ell} = V \otimes V \otimes \cdots \otimes V$ looks like $T = \sum_j v_{1j} \otimes v_{2j} \otimes \cdots \otimes v_{\ell j}$ for $(v_{1j}, v_{2j}, v_{3j}, \ldots, v_{\ell j}) \in V^\ell = V \times V \times \cdots \times V$.
  (a) If we write $v_{mj} = \sum_i c_{mji} e_i$, then $T = \sum_{1\le i_1,i_2,\ldots,i_\ell\le n} T^{i_1 i_2\cdots i_\ell} e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_\ell}$ where $T^{i_1 i_2\cdots i_\ell} = \sum_j \prod_{m=1}^{\ell} c_{mji_m}$.
  (b) Suppose that $\tilde{\mathbf{e}} = (\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_n)$ is another basis for V and let $(a_{ij}) = {}_{\tilde{\mathbf{e}}}[\mathrm{Id}_V]_{\mathbf{e}}$ denote the change of basis matrix. Show that $T = \sum_{1\le i_1,i_2,\ldots,i_\ell\le n} \tilde{T}^{i_1 i_2\cdots i_\ell} \tilde{e}_{i_1} \otimes \tilde{e}_{i_2} \otimes \cdots \otimes \tilde{e}_{i_\ell}$ where

$$\tilde{T}^{i_1 i_2\cdots i_\ell} = \sum_{1\le j_1,j_2,\ldots,j_\ell\le n} T^{j_1 j_2\cdots j_\ell} a_{i_1 j_1} a_{i_2 j_2} \cdots a_{i_\ell j_\ell}.$$

  (c) Conclude that T is a "(contravariant) tensor of rank ℓ".

In differential geometry and general relativity a k-tensor on a finite dimensional real vector space V is an element of $\mathrm{Mult}(V^k, \mathbb{R})$, the vector space of multilinear functions from $V \times V \times \cdots \times V$ to $\mathbb{R}$.

(183) In this Prompt a connection between tensors in general relativity/differential geometry and tensors in Math 593 is made.
  (a) Show $\mathrm{Mult}_{\mathbb{R}}(V^k, \mathbb{R}) \simeq (V^{\otimes k})^*$. [Hint: This is supposed to be easy.]
  (b) Show $\mathrm{Mult}_{\mathbb{R}}(V^k, \mathbb{R})$ is (canonically) isomorphic to $(V^*)^{\otimes k}$. [**Warning!** This is not true if V is infinite dimensional. Homework 155b may help.]
  (c) Conclude that a tensor in general relativity/differential geometry is a tensor in Math 593.

(184) (*Bonus*.) If you hang out with the differential geometry/general relativity crowd, you will notice they speak of (r,s)-tensors or "mixed tensors of type (r,s)". These are multilinear maps with r vector and s dual vector inputs which output a scalar. Show that such a map can naturally be identified with an element of

$$(V \otimes V \otimes \cdots \otimes V \otimes V^* \otimes V^* \otimes \cdots \otimes V^*)^*$$

where V occurs r times and V^* occurs s times. Show that this is, in turn, canonically isomorphic to $V^* \otimes V^* \otimes \cdots \otimes V^* \otimes V \otimes V \otimes \cdots \otimes V$ where V^* occurs r times and V occurs s times.

(185) (*Bonus.*) A mixed tensor of type (r,s) can be encoded as a quantity with $r+s$ indices, e.g. $A^{\mu_1\mu_2\cdots\mu_r}_{\nu_1\nu_2\cdots\nu_s}$, whose Cartesian components $\tilde{A}^{\mu_1\mu_2\cdots\mu_r}_{\nu_1\nu_2\cdots\nu_s}$ in a new coordinate system are obtained from the original ones by the rule

$$\tilde{A}^{\mu_1\mu_2\cdots\mu_r}_{\nu_1\nu_2\cdots\nu_s} = ????$$

What is ???? ? If your answer doesn't involve a transpose inverse somewhere, it is probably wrong.

(186) Suppose R is a commutative ring and M is a free R-module of free rank r. Show that $\bigwedge^d_R(M)$ is a free R module of free rank $\binom{r}{d}$.

(187) Show that for all R-modules Q and all $f \in \mathrm{Alt}^d_R(M,Q)$ there exists a unique $\bar{f} \in \mathrm{Hom}_R(\bigwedge^d_R(M), Q)$ for which the following diagram commutes.

$$\begin{array}{ccc} M^d & \xrightarrow{\wedge^d} & \bigwedge^d_R(M) \\ & \searrow^{f} & \downarrow \bar{f} \\ & & Q \end{array}$$

Every function f in $\mathrm{Sym}^d_R(M,\cdot)$ is a multilinear function that is characterized by the property that

$$f(m_1, m_2, \ldots, m_d) - f(m_{\tau(1)}, m_{\tau(2)}, \ldots, m_{\tau(d)}) = 0$$

for all involutions τ of $\mathbb{N}_d = \{1, 2, \ldots, d\}$. Thus, in creating a universal object that corresponds to $\mathrm{Sym}^d_R(M,\cdot)$ we should consider the R-submodule

$$Y = \langle (m_1 \otimes m_2 \otimes \cdots \otimes m_d) - (m_{\tau(1)} \otimes m_{\tau(2)} \otimes \cdots \otimes m_{\tau(d)}) \mid \text{for all } m_1 \otimes m_2 \otimes \cdots \otimes m_d \in M^{\otimes d} \text{ and all involutions } \tau \text{ of } \mathbb{N}_d \rangle$$

of $M^{\otimes d}$ and our candidate universal object is the quotient module $S^d_R(M) = M^{\otimes d}/Y$, which is called the *$d^{th}$ symmetric power module*. The induced map

$$\cdot^d \colon M^d \xrightarrow{\otimes^d} M^{\otimes d} \longrightarrow S^d_R(M)$$

is symmetric,[1] and the image of $(m_1, m_2, \ldots, m_d) \in M^d$ under this map is denoted $m_1 \cdot m_2 \cdot \cdots \cdot m_d$.

(188) Show that for all R-modules Q and all $f \in \mathrm{Sym}^d_R(M,Q)$ there exists a unique $\bar{f} \in \mathrm{Hom}_R(S^d_R(M), Q)$ for which the following diagram commutes.

$$\begin{array}{ccc} M^d & \xrightarrow{\cdot^d} & S^d_R(M) \\ & \searrow^{f} & \downarrow \bar{f} \\ & & Q \end{array}$$

(189) Suppose k is a field and V is an n-dimensional k-vector space.

(a) Show that the k-vector space $S^2(V)$ has dimension $\binom{n+1}{2}$. Show that the k-vector space $S^2(V^*)$ may be realized as the k-vector space of homogeneous of degree two polynomials (in n variables) on V. [A homogeneous of degree d polynomial in n variables has the property that $f(ta_1, ta_2, ta_3, \ldots, ta_n) = t^d f(a_1, a_2, \ldots, a_n)$. A polynomial p in n variables on V is function on V that for every basis $\beta = (v_1, v_2, \ldots, v_n)$ has the property that $p(x_1v_1 + x_2v_2 + \cdots + x_nv_n)$ is a polynomial in $x_1, x_2, \ldots, x_n$. If you've never checked before, you should check that being homogeneous of degree d is independent of the choice of basis.]

(b) (*Bonus.*) Show that the k-vector space $S^d(V)$ has dimension $\binom{n+d-1}{d}$. Show that the k-vector space $S^d(V^*)$ may be realized as the k-vector space of homogeneous of degree d polynomials in n-variables.

(190) Compute the rank and signature of the symmetric real matrix

$$\begin{bmatrix} -15 & -18 & -23 \\ -18 & -21 & -28 \\ -23 & -28 & -35 \end{bmatrix}$$

(191) Let V be the $\mathbb{R}$-vector space of all polynomials $ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$. For $p(x), q(x) \in V$, define

$$\langle p(x), q(x) \rangle = p'(0)q(0) + p(0)q'(0).,$$

where $p'(x)$ denotes the derivative of $p(x)$.

(a) Verify that $\langle\ ,\ \rangle$ is a symmetric bilinear form.

[1] Note that Y is the smallest submodule of $M^{\otimes d}$ for which the induced map from M^d to $M^{\otimes d}/Y$ is symmetric.

(b) Find an orthogonal basis of V with respect to $\langle\ ,\ \rangle$.
(c) What is the signature of $\langle\ ,\ \rangle$?

(192) Suppose $m \in \mathbb{Z}_{>1}$ and $I \leq \mathbb{Z}/(m)$ is an ideal.
(a) Show that there exists $k \in \mathbb{Z}$ with $k \mid m$ such that $I = k\mathbb{Z}/(m)$. Conclude that if $d = \frac{m}{k}$, then $I =_d \mathbb{Z}/(m) = \{x \in \mathbb{Z}/(m) \,|\, dx = 0\}$.
(b) Suppose $f \in \mathrm{Hom}_{\mathbb{Z}/(m)}(I, \mathbb{Z}/(m))$. Show that there exists $\ell \in \mathbb{Z}/(m)$ for which $f(i) = \ell i$ for all $i \in I$. Conclude that there exists $\tilde{f} \in \mathrm{Hom}_{\mathbb{Z}/(m)}(\mathbb{Z}/(m), \mathbb{Z}/(m))$ for which $\mathrm{res}_I\, \tilde{f} = f$.
(c) Show that $\mathbb{Z}/(m)$ is an injective $\mathbb{Z}/(m)$-module. [Hint: Imitate the proof of Homework 161.]
(d) (*Bonus.*) More generally, if R is a PID and $a \in R$, show $R/(a)$ is an injective $R/(a)$-module. [Hint: Copy the proof of Homework 161.]

(193) Suppose that A is a $\mathbb{Z}$-module.
(a) Show there is a surjective $\mathbb{Z}$-module homomorphism $\mathbb{Z}^{\oplus A} \to A$; conclude that $A \simeq \mathbb{Z}^{\oplus A}/K$ for some $\mathbb{Z}$-module $K \leq \mathbb{Z}^{\oplus A}$.
(b) Show that $\mathbb{Q}^{\oplus A}/K$ is injective. [Hmmmm. Proving essentially the same thing thrice (see Homework 161 and Homework 192); maybe there is a general result lurking here? It is called Baer's criterion; however, you do not need it to do this problem.]
(c) Conclude that every $\mathbb{Z}$-module may be identified with a submodule of an injective $\mathbb{Z}$-module.

Math 593. Homework 10b (Due November 19)

(194) Recall that in $\mathbb{R}^2$ the composition of two rotations is a rotation. Euler proved that the composition of two rotations (about possibly different axes) in $\mathbb{R}^3$ is also a rotation (around some third line through the origin). Your turn.
(a) Suppose that $R \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$. Show that $R \in \mathrm{SO}(\mathbb{R}^2, \cdot)$ if and only if R is a rotation about the origin. (Hint: Suppose that $\mathbf{v}$ is an orthonormal basis for $\mathbb{R}^2$, compute ${}_{\mathbf{v}}[R]_{\mathbf{v}}$.)
(b) Let L be a rotation in $\mathbb{R}^3$ by an angle θ about a line ℓ passing through the origin. Show that $L \in \mathrm{SO}(\mathbb{R}^3, \cdot)$. (Hint: find the matrix of L in a suitable basis.)
(c) Let L_1 and L_2 be two rotations in $\mathbb{R}^3$ about possibly different axes. Show that $M = L_1 \circ L_2 \in \mathrm{SO}(\mathbb{R}^3, \cdot)$.
(d) Show that 1 is an eigenvalue of M. (Hint: show $\det(M - I) = \det((M - I)^*) = -\det(M - I)$ using the fact that $MM^* = I$.)
(e) Let v be an eigenvector of M for the eigenvalue 1. Let W be the plane (through the origin) orthogonal to v. Show that $M(W) = W$ and that $\mathrm{res}_W\, M \in \mathrm{O}(W, \cdot)$.
(f) Show that $\mathrm{res}_W\, M \in \mathrm{SO}(W, \cdot)$.
(g) Conclude that M is a rotation in $\mathbb{R}^3$ about a line through the origin.
(h) Is every element of $\mathrm{SO}(\mathbb{R}^3, \cdot)$ given by rotation about a line through the origin? What do elements of $\mathrm{O}(\mathbb{R}^3, \cdot)$ look like?
(i) Let L_1 be rotation about the x-axis by an angle of 90° which sends the y-axis to the z-axis and L_2 a rotation about the y-axis by an angle of 90° which sends the z-axis to the x-axis. Let $M = L_1 \circ L_2$. Then M is a rotation about what line? By what angle?
(j) Bonus: Now do the same problem with the angles 90° replaced by 45°.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 11a (Due November 23)

Thanksgiving – no homework

Math 593. Homework 11b (Due November 26)

(195) Recall how to compute (that is, remember what matrices are for). Let V denote the subspace of $C^\infty(\mathbb{R})$ spanned by $\sin(t)$, $t\sin(t)$, $\cos(t)$, and $t\cos(t)$.

(a) Show that $\mathcal{B} = (\sin(t), t\sin(t), \cos(t), t\cos(t))$ is a basis for V.

(b) Show that if $f \in V$, then $f' \in V$. Thus, we can define $D \in \mathrm{Hom}_{\mathbb{R}}(V, V)$ by $D(f) = f'$ for $f \in V$.

(c) Let $A \in \mathbb{R}^{4\times 4}$ denote the $\mathcal{B}$-matrix of D; that is, $A = {}_{\mathcal{B}}[D]_{\mathcal{B}}$. Compute A. For the rest of this problem, you are not allowed to compute any derivatives or integrals.

(d) Show that $A^4 + 2A^2 + I_4 = 0$. Conclude that A is invertible and compute A^{-1}.

(e) Use A^{-1} to compute an antiderivative of $17\sin(x) - 4x\cos(x) + 9x\sin(x)$. Explain, without computing any integrals or derivatives, how you know your answer is correct.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 12a (Due November 30)

(196) Suppose k is $\mathbb{R}$ or $\mathbb{C}$, V is a k-vector space, and $\langle\ ,\ \rangle$ is an inner product on V. For $v \in V$ define the *norm* of v, denoted $\|v\|$, by $\|v\| = \sqrt{\langle v, v\rangle}$. One should think of $\|v\|$ as the length of v. Show

(a) For all $v, w \in V$ we have

$$\|v \pm w\|^2 = \|v\|^2 \pm 2\,\mathrm{Re}(\langle v, w\rangle) + \|w\|^2.$$

(b) (polarization identity over $\mathbb{R}$) If $k = \mathbb{R}$, then for all $u, v \in V$ we have

$$\langle u, v\rangle = \frac{1}{4}\|u + v\|^2 - \frac{1}{4}\|u - v\|^2.$$

(c) (polarization identity over $\mathbb{C}$) if $k = \mathbb{C}$, then for all $u, v \in V$ we have

$$\langle u, v\rangle = \frac{1}{4}\sum_{m=k}^{4} i^m \|u + i^m v\|^2 = \frac{1}{4}\|u + v\|^2 - \frac{1}{4}\|u - v\|^2 + \frac{i}{4}\|u + iv\|^2 - \frac{i}{4}\|u - iv\|^2.$$

(d) (Cauchy-Bunyakovsky-Schwarz inequality) Suppose k is $\mathbb{R}$ or $\mathbb{C}$. show that for all $u, v \in V$ we have

$$|\langle u, v\rangle| \leq \|u\|\|v\|.$$

[Hint: Draw a picture of the situation in $\mathbb{R}^2$ with the standard inner product. Show that we can reduce to the case when $\|u\| = 1$ and look at the vector $w = v - \langle v, u\rangle u$. Square everything.]

(e) (triangle inequality) Suppose k is $\mathbb{R}$ or $\mathbb{C}$. show that for all $u, v \in V$ we have

$$\|u + v\| \leq \|u\| + \|v\|.$$

[Hint: Square everything.]

(197) (Bessel's inequality) Suppose k is $\mathbb{R}$ or $\mathbb{C}$, V is a k-vector space, and $\langle\ ,\ \rangle$ is an inner product on V.

(a) Suppose $(u_1, u_2, \ldots, u_k)$ is an orthogonal set of non-zero vectors in V. If v is any vector in V, then

$$\sum_{m=1}^{k} \frac{|\langle v, u_m\rangle|^2}{\|u_m\|^2} \leq \|v\|^2$$

with equality if and only if

$$v = \sum_{m=1}^{k} \frac{\langle v, u_m\rangle}{\|u_m\|^2} u_m.$$

(b) Show

$$\int_0^1 \left|\sum_{n=-k}^{k} c_n e^{2\pi i n t}\right|^2 dt = \sum_{n=-k}^{k} |c_n|^2.$$

(c) Show that for all $f \in C^0([0,1], \mathbb{C})$ we have

$$\sum_{n=-k}^{k} \left|\int_0^1 f(t) e^{-2\pi i n t}\, dt\right|^2 \leq \int_0^1 |f(t)|^2\, dt.$$

(198) Suppose k is $\mathbb{R}$ or $\mathbb{C}$, V is a finite dimensional k-vector space, and $\langle\ ,\ \rangle$ is an inner product on V. Let W be a subspace of V. Show that $V = W + W^\perp$ and $W \cap W^\perp = \{0\}$.

(199) Suppose k is a field, V is a finite dimensional k-vector space, and $B \in \mathrm{Bil}(V^2, k)$ is alternating. Show that there exists a basis $\mathbf{v}$ for V such that the matrix $M = M(B, \mathbf{v})$ of B with respect to $\mathbf{v}$ is of the form $M = \mathrm{diag}(S, S, S, \ldots, S, 0, 0, \ldots, 0)$ where $S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

(200) Suppose k is a field, V is a finite dimensional k-vector space, and $B \in \mathrm{Bil}(V^2, k)$ is alternating. Show that the rank of B is even and its determinant is a square. [Hint: Homework 199.]

(201) Suppose k is a field and V is a finite dimensional k-vector space. Suppose $B, B' \in \mathrm{Bil}(V^2, k)$ are alternating. Show that B and B' are cogredient if and only if they have the same rank. [Hint: Homework 199.]

(202) Show that the sequence that occurs prior to Prompt 317 is exact at $\ker(h)$.

Definition. Suppose R is a ring. A *cochain complex of R-modules* is a sequence of R-modules and R-module homomorphisms

$$\cdots \xrightarrow{d^{i-2}} M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \xrightarrow{d^{i+1}} \cdots$$

such that $d^i \circ d^{i-1} = 0$ for all i. The cochain complex is often denoted $M^\bullet$ or $(M^\bullet, d^\bullet)$.

(203) Show that by setting $M_j = M^{-j}$ and $d_j = d^{-j}$ every cochain complex may be viewed as a chain complex. Is the converse true?

Definition. Suppose $M^\bullet$ is a cochain complex of R-modules. The *i^{th} cohomology of $M^\bullet$* is the R-module $\mathrm{H}^i(M^\bullet) := \ker(d^i)/\operatorname{im}(d^{i-1})$.

(204) Show that $\mathrm{H}_j(M_\bullet) = \mathrm{H}^{-j}(M^{-\bullet})$.

Definition. Suppose R is a ring and N is an R-module. A *(left) resolution* of N an exact sequence

$$\cdots \longrightarrow Q^{-n} \longrightarrow Q^{1-n} \longrightarrow \cdots\cdots \longrightarrow Q^{-1} \longrightarrow Q^0 \longrightarrow N \longrightarrow 0$$

where each Q^m is an R-module. A resolution is said to be *finite* provided that only finitely many of the modules Q^m are nonzero.

We should call this a *coresolution*, but almost nobody does.

(205) Suppose R is a ring and N is an R-module. Show that

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots\cdots \longrightarrow 0 \longrightarrow N \longrightarrow N \longrightarrow 0$$

is a resolution of N. The goal is to use resolutions to learn something about N, so we usually require the elements Q^j of our cochain to be special in some way (e.g., they are all free, or projective, or injective, or ...). Typically, N will not be required to be special.

We often abuse language and say that the cochain complex $Q^\bullet$ given by

$$\cdots \longrightarrow Q^{-n} \longrightarrow Q^{1-n} \longrightarrow \cdots\cdots \longrightarrow Q^{-1} \longrightarrow Q^0 \longrightarrow 0$$

is a resolution of N. The only change is at the tail: the sequence $Q^0 \longrightarrow N \longrightarrow 0$ has been changed to $Q^0 \longrightarrow 0$. Note that this is still a complex, sometimes called a *deleted complex*, it just is no longer exact.

(206) Show

$$\mathrm{H}^j(Q^\bullet) \simeq \begin{cases} 0 & j \neq 0 \\ N & j = 0. \end{cases}$$

(207) Suppose R is a commutative ring and M is an R-module. From Homework 193 we know that there is an injective $\mathbb{Z}$-module Q so that M is a $\mathbb{Z}$-submodule of Q. Show that

$$M \simeq \operatorname{Hom}_R(R, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(R, Q).$$

Conclude that M may be identified with a submodule of an injective R-module. [Hint: Use Homework 175.]

(208) Suppose that R is a ring. Suppose M is an R-module. Show that the following are equivalent.
- (a) M is projective
- (b) M is a direct summand of a free R-module. That is, there exists a free R-module F that contains M and a submodule K of F so that $F = K \oplus M$.

(209) Suppose R is a PID and M is an R-module. Show that M is projective if and only if M is free. [Hint: Use Homework 208 and Homework 121. For a proof of Homework 121 see [Lan02, pp. 880–881].]

Math 593. Homework 12b (Due December 3)

(210) Spectral Theorem over $\mathbb{R}$. Suppose that $(V, \langle\ ,\ \rangle)$ is a nonzero finite dimensional real inner product space.
- (a) Suppose $T \in \operatorname{End}(V)$. If there is an orthonormal basis of V which consists of eigenvectors of T, then T is self-adjoint.

(b) The converse to (210a) is also true, and it is called the *spectral theorem for self-adjoint operators*. The rest of this problem develops a 'geometric' proof of this result. For the rest of this problem, we suppose that $T \in \mathrm{Hom}(V, V)$ is self-adjoint. Show that if $v, w \in V$ are eigenvectors for T with distinct eigenvalues, then $\langle v, w\rangle = 0$.

(c) Suppose that $v \in V$ is an eigenvector for T. Show that if $W = v^{\perp} := \{v' \in V \mid \langle v', v\rangle = 0\}$, then $\mathrm{res}_W T$, the restriction of T to W, belongs to $\mathrm{Hom}_{\mathbb{R}}(W, W)$ and is self-adjoint.

(d) Show that if every self-adjoint operator S on an inner product space $(V', \langle\ ,\ \rangle')$ has an eigenvector, then the spectral theorem is true for T.

(e) Show that the map from V to $\mathbb{R}$ sending $v \in V$ to $\|v\|$ is continuous.

(f) Let $S = \{v \in V \mid \|v\| = 1\}$. Show that S is compact in V.

(g) Show that $Q_T \colon S \to \mathbb{R}$ defined by $Q_T(v) = \langle T(v), v\rangle$ is (uniformly) continuous. (Hint, you may want to show that there is a constant $c_T \in \mathbb{R}$ such that $\|T(v)\| \leq c_T\|v\|$ for all $v \in V$.)

(h) Show there is a $v_0 \in S$ such that $Q_T(v_0) \geq Q_T(v)$ for all $v \in S$. Set $\lambda_T := Q_T(v_0)$.

(i) We now show that $T(v_0) = \lambda_T(v_0)$; that is T does have an eigenvector, and so the spectral theorem is true! Suppose $T(v_0) \neq \lambda_T(v_0)$.

  (i) Since $w = T(v_0) - \lambda_T v_0$ is not zero we may define $v_1 = w/\|w\|$. Show that v_1 is perpendicular to v_0.

  (ii) Let $W = \mathrm{span}(v_0, v_1)$. Show that $T(v_0) \in W$.

  (iii) Show that for every $t \in \mathbb{R}$ we have $\cos(2\pi t)v_0 + \sin(2\pi t)v_1 \in S \cap W$.

  (iv) Define $f \colon \mathbb{R} \to \mathbb{R}$ by $f(t) = Q_T(v_t)$. Use elementary calculus to show that v_1 is perpendicular to $T(v_0)$.

  (v) Conclude that we must have $T(v_0) = \lambda_T(v_0)$.

Please report any errors you find to smdbackr@umich.edu

Math 593. Homework 13a (Due December 7)

(211) Suppose $m \in \mathbb{Z}_{>1}$ and N is a $\mathbb{Z}$-module. Compute $\operatorname{Tor}_i^{\mathbb{Z}}(N, \mathbb{Z}/(m))$. Compare your answer with your response to Prompt 328.

(212) Suppose R is a commutative ring. Show that every projective R-module is flat.

(213) Suppose R is a commutative ring, $D \subset R$ is multiplicatively closed, and M is an R-module. For $(d, m), (d', m') \in D \times M$ we write $(d, m) \sim (d', m')$ provided that

$$r(dm' - d'm) = 0 \text{ for some } r \in D.$$

This is an equivalence relation, and the resulting set of equivalence classes is denoted $D^{-1}M$. We call $D^{-1}M$ the *localization of M at D*.

(a) Verify that $D^{-1}M$ is a $D^{-1}R$-module. Formulate a universal property for it.

(b) Show that $D^{-1}M \simeq D^{-1}R \otimes_R M$.

(c) Prove that localization commutes with tensor products. That is, show that for all R-modules L and N there is a unique isomorphism of $D^{-1}R$-modules $\varphi\colon D^{-1}L \otimes_{D^{-1}R} D^{-1}N \simeq D^{-1}(L \otimes_R N)$ with $\varphi(\ell/d \otimes n/d')$ given by $\ell \otimes n/dd'$.

(214) Suppose R is a ring. Show that the following conditions on an R-module M are equivalent.

- M is projective.
- $\operatorname{Ext}_R^1(M, N) = 0$ for all R-modules N.
- $\operatorname{Ext}_R^n(M, N) = 0$ for all n and all R-modules N.

[Hint: Use Prompt 331.]

(215) Suppose that R is a ring and $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence of R-modules. Let $0 \longrightarrow L \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots$ and $0 \longrightarrow M \longrightarrow J^0 \longrightarrow J^1 \longrightarrow \cdots$ be injective resolutions of L and N, respectively.

(a) Show that for each n we have $I^n \oplus J^n$ is an injective R-module. *Warning:* In general, the direct product of injectives modules is injective, but the direct sum of injectives need not be injective. Thankfully, in the category of R-modules, finite direct sums and finite direct products coincide.

(b) Show that $0 \longrightarrow M \longrightarrow I^0 \oplus J^0 \longrightarrow I^1 \oplus J^1 \longrightarrow \cdots$ is an injective resolution of M such that the following diagram has exact columns, exact rows, and commutes.

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & I^2 & \longrightarrow & I^2 \oplus J^2 & \longrightarrow & J^2 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & I^1 & \longrightarrow & I^1 \oplus J^1 & \longrightarrow & J^1 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & I^0 & \longrightarrow & I^0 \oplus J^0 & \longrightarrow & J^0 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

(c) Conclude that if F is an additive left-exact functor from the category of R-modules to the category of $\mathbb{Z}$-modules, then we have a long exact sequence

$$\cdots \longrightarrow R^jF(N) \xrightarrow{\delta^j} R^{j+1}F(L) \longrightarrow R^{j+1}F(M) \longrightarrow R^{j+1}F(N) \xrightarrow{\delta^{j+1}} R^{j+2}F(L) \longrightarrow \cdots$$

that begins with

$$0 \longrightarrow F(L) \longrightarrow F(M) \longrightarrow F(N) \xrightarrow{\delta^0} R^1F(L) \longrightarrow \cdots$$

(216) Suppose $\ell \in \mathbb{Z}_{>0}$.
  (a) For $k \in \mathbb{Z}$ consider $\mu_k \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(\ell), \mathbb{Z}/(\ell))$ where $\mu_k(x) = kx$. Show that the image of μ_k is $\langle (k, \ell) \rangle$ and the kernel of μ_k has (k, ℓ) elements.
  (b) Use the left exactness of $Y \mapsto \mathrm{Hom}_{\mathbb{Z}}(Y, \mathbb{Z}/(\ell))$ and the exactness of $\mathbb{Z} \xrightarrow{\mu_k} \mathbb{Z} \longrightarrow \mathbb{Z}/(k) \longrightarrow 0$ to show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(k), \mathbb{Z}/(\ell)) \simeq \mathbb{Z}/(k, \ell)\mathbb{Z}$.

(217) Suppose R a commutative ring and $r \in R$ a non-zero-divisor. For an R-module N, let ${}_rN$ denote the R-module of r-torsion elements of N, that is, ${}_rN = \{n \in N \mid rn = 0\}$. Show that $\mathrm{Tor}_1^R(N, R/(r)) \simeq {}_rN$. Does this contradict your findings in Prompt 344?

(218) Suppose $R = \mathbb{Z}[x]/(x^k)$ is a commutative ring and $I = (x^\ell)$ is a principal ideal in R. Show

$$\mathrm{Tor}_i^R(I, M) = \begin{cases} {}_{x^\ell}M/x^{k-\ell}M & \text{if } i \neq 0 \text{ is even} \\ {}_{x^{k-\ell}}M/x^\ell M & \text{if } i \text{ is odd} \\ M/x^{k-\ell}M & \text{if } i = 0 \end{cases}$$

for an R-module M. Here ${}_{x^\ell}M = \{m \in M \mid x^\ell m = 0\}$.

(219) Suppose R is a ring and M and N are R-modules. Let $E(M, N)$ denote the set of extensions of M by N and recall that given $\tilde{E}_i = 0 \longrightarrow N \longrightarrow E_i \longrightarrow M \longrightarrow 0 \in E(M, N)$ for $i \in \{1, 2\}$ we say that $\tilde{E}_1$ is equivalent to $\tilde{E}_2$ (and we write $\tilde{E}_1 \sim \tilde{E}_2$) provided that there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E_1 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_N} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}_M} & & \\ 0 & \longrightarrow & N & \longrightarrow & E_2 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Let F be a free module with $\pi \in \mathrm{Hom}_R(F, M)$ a surjection. Set $K = \ker(\pi)$ and let $\iota \in \mathrm{Hom}_R(K, F)$ denote the natural inclusion of K in F. Fix $\kappa \in \mathrm{Ext}_R^1(M, N) \simeq \mathrm{coker}(\iota^*)$. [Why can we write $\mathrm{Ext}_R^1(M, N) \simeq \mathrm{coker}(\iota^*)$?] Choose $k \in \mathrm{Hom}_R(K, N)$ so that the image of k in $\mathrm{Ext}_R^1(M, N)$ is κ.
  (a) Let E denote the cokernel of the injective homomorphism $(\iota, k) \in \mathrm{Hom}_R(K, F \oplus N)$. Show that the surjection $(\pi, 0) \in \mathrm{Hom}_R(F \oplus N, M)$ factors through E giving us a surjective homomorphism $\bar{\pi} \in \mathrm{Hom}_R(E, M)$.
  (b) Show that the natural injective homomorphism $N \simeq \{0\} \oplus N \hookrightarrow F \oplus N$ given by $n \mapsto (0, -n)$ defines an injective homomophism $\varphi \in \mathrm{Hom}_R(N, E)$. Show that $\mathrm{im}(\varphi) = \ker(\bar{\pi})$.
  (c) Set $e(\kappa) = E \in E(M, N)$. Show that $e(\kappa)$ is independent of all of the choices above in the sense that different choices lead to equivalent extensions.
  (d) Recall the map $\bar{\nu} \colon E(M, N) \to \mathrm{Ext}_R^1(M, N)$ that was defined in Prompt 361.
    (i) Show that $\kappa = \bar{\nu}(e(\kappa))$
    (ii) Show that for $\tilde{E} \in E(M, N)$ we have $e(\bar{\nu}(\tilde{E})) \sim \tilde{E}$.
  (e) Conclude that $\mathrm{Ext}_R^1(M, N)$ measures the extensions of M by N up to natural equivalence.
  (f) Consider the $\mathbb{Z}/(18)$-modules $\mathbb{Z}/(6)$ and $\mathbb{Z}/(3) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(9)$. Up to equivalence, how many extensions of $\mathbb{Z}/(6)$ by $\mathbb{Z}/(3) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(9)$ are there?

(220) EROs and ECOs: Bruhat Decomposition. Suppose k is a field. Let B denote the subgroup of $\mathrm{GL}_n(k)$ consisting of matrices which are upper triangular (that is, if $A \in B$, then $A_{ij} = 0$ whenever $i > j$). The set B is actually a group, called a Borel subgroup of $\mathrm{GL}_n(k)$. It might be helpful to work out the following for $n = 1, 2, 3$ before trying to write down a general proof. Let $W \subset \mathrm{GL}_n(k)$ denote the set of permutation matrices ($A \in W$ if and only if each entry of A is either zero or one and each column and each row contains exactly one nonzero entry). Note that W has $n!$ elements and, in fact, is a group that is isomorphic to S_n.[1]
  (a) Establish the Bruhat decomposition: $\mathrm{GL}_n(k) = \sqcup_{w \in W} BwB$. [Hint: Many of the elementary row and column operations belong to B. Also, we have an equivalence relation on $\mathrm{GL}_n(\mathbb{R})$ defined by $x \sim y$ provided that there exist $b, b' \in B$ such that $bx = yb'$; the equivalence class of $z \in \mathrm{GL}_n(\mathbb{R})$ is the B-double coset BzB. The set of B-double cosets is denoted $B\backslash \mathrm{GL}_n(k)/B$.]

[1] The natural isomorphism takes $\sigma \in S_n$ to the unique element $w \in W$ for which $\prod w_{i\sigma(i)} \neq 0$. What is the determinant of this w? Make sure you understand this.

(b) For which $w \in W$ is

$$\begin{pmatrix} 9 & 5 & 7 \\ -9 & -6 & 9 \\ -3 & -2 & -1 \end{pmatrix}$$

in BwB?

(c) Is every element of $\mathrm{GL}_n(k)$ the product of elementary matrices?

(d) *Bonus*. Let $G = \mathrm{GL}_n(k)$. The group G acts on $G/B \times G/B$ by $g \cdot (xB, yB) = (gxB, gyB)$ for $x, y \in G$. Show that

$$G/B \times G/B = \bigsqcup_{w \in W} G \cdot (B, wB).$$

(221) Suppose R is a ring and M is an R-module. Suppose $r \in R$ is not zero and not a zero divisor. Show that $\mathrm{Tor}_1(M, R/(r))$ is isomorphic to the r-torsion of M, that is, the submodule of elements of $m \in M$ for which $rm = 0$. [This is why Tor is called Tor.] Does this contradict your findings in Prompt 344?

(222) Suppose that I and J are ideals in a commutative ring R. In Prompt 27 we decided that if I and J are comaximal, then $IJ = I \cap J$. However, we also noticed that the converse is not true. Show that $IJ = I \cap J$ if and only if $\mathrm{Tor}_1(R/I, R/J) = 0$. [Hint: Start with the exact sequence $0 \to I \to R \to R/I \to 0$.]

(223) Show that the sequence that occurs prior to Prompt 317 is exact at $\mathrm{coker}(f)$.

(224) Suppose R is a commutative ring. Show that the ring of Laurent polynomials on R, denoted $R[x, x^{-1}]$, is the localization of the polynomial ring $R[x]$ at $D = \{x, x^2, x^3, \ldots\}$. [This is $R[x]_x$ in the notation of Prompt 38.]

Math 593. Homework 13b (Due December 10)

(225) Exactly one of the following two-by-two matrices with entries in $\mathbb{R}$ is diagonalizable over $\mathbb{R}$, call it A.

$$\begin{bmatrix} -22 & 484 \\ -1 & 22 \end{bmatrix} \qquad \begin{bmatrix} 22 & 21 \\ -21 & 22 \end{bmatrix} \qquad \begin{bmatrix} 22 & -21 \\ -21 & 22 \end{bmatrix}$$

(a) Find an eigenbasis for A.

(b) Produce a diagonal matrix D and a change of coordinates matrix M so that $A = MDM^{-1}$.