WORKSHEETS FROM MATH 593: ALGEBRA I, UNIVERSITY OF MICHIGAN, FALL 2021

These are the worksheets from a graduate algebra course focusing on rings and modules, taught at the University of Michigan in Fall 2021. The worksheets were written by David E Speyer, based on earlier worksheets by Stephen DeBacker. If you wish to use them for teaching, contact David E Speyer (speyer@umich.edu) for the LaTeX source; I will probably be glad to send it to you.

Many thanks to the students, Emilee Cardin, Thomas Cohn, Heitor Anginiski Cotosky, Zach Deiman, Ram Ekstrom, Taeyoung Em, Yuqin Kewang, Jose Alan Esparaza Lorenzo, Sandra Nair, Urshita Pal, Mia Smith and Matthew Wang for their work and suggestions.

CONTENTS

WORKSHEET 1: RINGS

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***)

and elements 0_R and 1_R satisfying [1]the following axioms:

R1: $(R, +, 0_R)$ 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: $1_R * r = r * 1_R = r$ for all $r \in R$.

We will almost always drop the symbol $*$ and write ab for $a * b$; similarly, we will write 0 and 1 for 0_R and 1_R. A ring is said to be ***commutative*** provided that its multiplicative operation is commutative.[2] A ***zero ring*** is a ring with one element.

Problem 1.1. Suppose R is a ring. Show $\mathrm{Mat}_{n\times n}(R)$ is a ring with respect to matrix multiplication.

Problem 1.2. Let G be a group and k a ring. The ***group ring*** kG is defined to be the set of sums of the form $\sum_{g\in G} a_g g$, where the a_g are in k and all but finitely many a_g are 0, with the "obvious" addition and multiplication. Spell out what the "obvious" definitions are and check that they are a ring.

Problem 1.3. Let A be an abelian group. Let $R = \mathrm{Hom}_{\mathrm{grp}}(A, A)$, and define operations $+$ and $*$ on R by $(r_1 + r_2)(a) = r_1(a) + r_2(a)$ and $(r_1 * r_2)(a) = r_1(r_2(a))$. Show that R is a ring.

This ring is called the ***endomorphism*** ring of A and denoted $\mathrm{End}(A)$.

Problem 1.4. Why did we require that A was abelian in the previous problem?

Problem 1.5. Suppose R is a ring. Show that $0_R * x = x * 0_R = 0_R$ for all $x \in R$.

Problem 1.6. Suppose that R is a ring with $0_R = 1_R$. Show that R is the zero ring.

Definition. Suppose that R is a ring. An element $u \in R$ is called a ***unit*** if there is an element u^{-1} with $u * u^{-1} = u^{-1} * u = 1_R$. The set of units of R is denoted $R^\times$.

Problem 1.7. Show that $R^\times$ is a group with respect to $*$.

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[3]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 $\mathrm{Hom}_{\mathrm{ring}}(R, S)$.

Problem 1.8. Let $R = \mathbb{Z}/15\mathbb{Z}$ and let $S = \mathbb{Z}/3Z$. What is $\mathrm{Hom}_{\mathrm{ring}}(R, S)$? What about $\mathrm{Hom}_{\mathrm{ring}}(S, R)$? What if we allow non-unital homomorphisms?

Problem 1.9. We defined a group ring above. For those who know what a monoid and/or a category are: Can you define a ***monoid ring***? What about a ***category ring***?

---

[1]Some people do not impose that a ring has a multiplicative identity, but in this course all rings will have a multiplicative identity. See Poonen, "Why all rings should have a 1", `https://math.mit.edu/~poonen/papers/ring.pdf` for an argument. A ring without an identity is sometimes called a ***rng***. A ring without negatives is sometimes called a ***rig***.

[2]A commutative ring is sometimes called a ***grin***. Actually, no one does this, but they should!

[3]Some people do not impose that $f(1_R) = 1_S$. These people call f ***unital*** when $f(1_R) = 1_S$. In this course, we define homorphisms to be unital, and say "non-unital homomorphism" on the rare occasions that we need this concept.

WORKSHEET 2: MODULES

Groups are meant to act on sets. Similarly, rings are meant to act on abelian groups.

Definition: 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***)

and an element 0_M satisfying the following axioms:

M1: $(M, +, 0_M)$ 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: $1_R * m = m$ for all $m \in M$.[1]

"*M **is an** R**-module***" will mean "M is a left R-module".

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***.

Problem 2.1. Show that $\mathbb{Z}^n$ is a left-$\mathrm{Mat}_{n\times n}(\mathbb{Z})$-module by having $X \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ act on $\mathbb{Z}^n$ by taking $v \in \mathbb{Z}^n$ to Xv.

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 $\mathrm{Hom}_R(M,N)$. We set $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$ and call $\mathrm{End}_R(M)$ the ***endomorphism ring of*** M.

Problem 2.2. Suppose R is a commutative ring and M is an R-module. Show that there is a "natural" map of rings $R \to \mathrm{End}_R(M)$. What if R is not commutative?

Definition. Suppose R is a ring and M and N are R-modules. The ***direct sum*** of M and N, written $M \oplus N$, is the R-module defined as follows: An element of $M \oplus N$ is an ordered pair (m,n) with $m \in M$ and $n \in N$. We have $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$ and $r(m,n) = (rm, rn)$.

Problem 2.3. Check that $M \oplus N$ is an R-module.

Problem 2.4. Let M_1, M_2, M, N_1, N_2 and N be R-modules. Show that $\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong \mathrm{Hom}_R(M_1, N) \times \mathrm{Hom}_R(M_2, N)$ and $\mathrm{Hom}_R(M, N_1 \oplus N_2) \cong \mathrm{Hom}_R(M, N_1) \times \mathrm{Hom}_R(M, N_2)$ as abelian groups.

Problem 2.5. Let $L_1, L_2, \ldots, L_p$, $M_1, M_2, \ldots, M_q$ and $N_1, N_2, \ldots, N_r$ be R-modules, and let $L = \bigoplus L_i$, $M = \bigoplus M_j$ and $N = \bigoplus N_k$. Describe a way to write elements of $\mathrm{Hom}_R(L,M)$, $\mathrm{Hom}_R(M,N)$ and $\mathrm{Hom}_R(L,N)$ as matrices, so that the composition map $\mathrm{Hom}_R(L,M) \times \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(L,N)$ corresponds to matrix multiplication.

[1] As you might guess, some people do not impose this last condition.

WORKSHEET 3: IDEALS

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 a ***two-sided ideal***.

If R is commutative, then "left ideal", "right ideal" and "two-sided ideal" are the same, and we will simply write ***ideal***. [1]

Problem 3.1. Show that if A and B are ideals, then $A + B := \{a + b : \ a \in A, \ b \in B\}$ is also an ideal.

Problem 3.2. Fix $n \geq 2$. Let I be the subset of $R = \mathrm{Mat}_{n \times n}(\mathbb{Q})$ consisting of matrices with nonzero entries only in the first row. Is I a left ideal? Is it a right ideal?

Problem 3.3. Suppose R and S are rings and $\varphi \in \mathrm{Hom}(R, S)$. Show that $\ker(\varphi)$ is a two-sided ideal of R.

Problem 3.4. Let R be a ring and let I be a left ideal. Since I and R are abelian groups with respect to $+_R$, we can form the quotient group R/I. Show that R/I has a natural structure as a left R-module.

Problem 3.5. Let R be a ring and let I be a two sided ideal. Show that R/I has a natural ring structure.

[1] In this course, we will not use the word "ideal" in a non-commutative ring without saying whether it is a left ideal, right ideal or two-sided ideal. If you see a source using "ideal" by itself in a non-commutative setting, it probably means "two-sided ideal", but Prof. Speyer recommends being clearer and not using the word "ideal" by itself in this context.

WORKSHEET 4: INTEGRAL DOMAINS

Definition: A commutative ring R is called an ***integral domain*** if:

ID1: Whenever $xy = 0$ in R, we have either $x = 0$ or $y = 0$ and
ID2: The ring R is not the zero ring.

Integral domains are similar to fields, but not as nice. The next problems explore the relationship.

Problem 4.1. Show that a field is an integral domain.

Problem 4.2. Show that $\mathbb{Z}$ is an integral domain but not a field.

Problem 4.3. Show that $k[x]$ is an integral domain but not a field, where k is a field.

Problem 4.4. Let R be a nonzero commutative ring.

(1) Show that R is an integral domain if and only if, for all $x \neq 0$ in R, the map $y \mapsto xy$ is injective.
(2) Show that R is a field if and only if, for all $x \neq 0$ in R, the map $y \mapsto xy$ is bijective.

Problem 4.5. Let R be an integral domain and suppose that $\#(R)$ is finite. Show that R is a field.

Problem 4.6. Let R be an integral domain and let k be a subring of R which is a field, such that R is finite dimensional as a k-vector space. Show that R is a field.

Every integral domain R embeds in a natural field, known as the ***field of fractions of*** R and denoted $\mathrm{Frac}(R)$.

Definition: Let R be an integral domain. Define X to be the set of pairs (p, q) in R^2 with $q \neq 0$. Define an equivalence relation $\sim$ on X by

$$(p_1, q_1) \sim (p_2, q_2) \text{ if and only if } p_1 q_2 = p_2 q_1.$$

We will denote an element of $X/\sim$ as p/q or $\frac{p}{q}$. We define addition and multiplication on $X/\sim$ by:

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} \qquad \frac{p_1}{q_1} * \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2}.$$

We denote this field $\mathrm{Frac}(R)$.

Problem 4.7. Verify that $\sim$ is an equivalence relation on X.

Problem 4.8. Verify that $X/\sim$ is a field under the operations $+$ and $*$ on $X/\sim$.

At this point, we can see why it is a good idea to define $\{0\}$ **not** to be an integral domain: If we try these definitions with $R = \{0\}$, then $X = \emptyset$, so $\mathrm{Frac}(R)$ would be $\emptyset$ and, in particular, would not have additive or multiplicative identities.

Worksheet 5: Prime and Maximal Ideals

Definition: Suppose R is a commutative ring. An ideal P of R is called ***prime*** if,

P1: for all a and $b \in R$, if $ab \in P$ then $a \in P$ or $b \in P$.
P2: The ideal P is not all of R.

Problem 5.1. Let R be a commutative ring; let I be an ideal of R. Show that I is prime iff R/I is an integral domain.

Problem 5.2. For which integers n is $n\mathbb{Z}$ prime? You may assume uniqueness of prime factorization for this question. [1]

Definition: Suppose R is a commutative ring. An ideal $\mathfrak{m}$ of R is called ***maximal*** if:

M1: For all a in R, if $a \notin \mathfrak{m}$ then there is some $b \in R$ such that $ab \equiv 1 \bmod \mathfrak{m}$.
M2: The ideal $\mathfrak{m}$ is not all of R.

Problem 5.3. Let R be a commutative ring and let I be an ideal of R. Show that I is maximal and only if R/I is a field.

Problem 5.4. Show that a maximal ideal is prime.

Problem 5.5. Show that an ideal $I \subsetneq R$ is maximal if and only there does not exist an ideal J with $I \subsetneq J \subsetneq R$.

Problem (5.5) is the motivation for the word "maximal". Using Zorn's lemma, and Problem (5.5), it is easy to show that every ideal in a nonzero commutative ring is contained in a maximal ideal.

Problem 5.6. Let $R = \mathbb{R}[x, y]$. Show that yR is prime but not maximal.

Problem 5.7. Let R be a commutative ring and let P be a prime ideal. Suppose that R/P is finite. Show that P is maximal.

Problem 5.8. What are the maximal ideals of $\mathbb{Z}$?

[1] Pretty soon, we will discuss unique factorization in commutative rings in general. At that point, we will prove it for $\mathbb{Z}$ (and many other rings). The careful student can check that there is no circularity; the problems where I permit you to use it now will not feed into our proof then.

WORKSHEET 6: PRODUCTS OF RINGS AND MODULES

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
- $(r,s) * (r',s') = (r * r', s * s')$ for all $(r,s), (r',s') \in R \times S$.

Problem 6.1. Show that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/15\mathbb{Z}$ are isomorphic as rings.

Problem 6.2. Are there natural ring homomorphisms $R \to R \times S$ and $S \to R \times S$? Are there natural ring homomorphisms $R \times S \to R$ and $R \times S \to S$?

Problem 6.3. Let R and S be rings and let M and N be an R-module and an S-module respectively. Explain how to put an $(R \times S)$-module structure on the abelian group $M \times N$.

Every $(R \times S)$-module breaks up as in Problem 6.3, as the next problem explains.

Problem 6.4. Let R and S be rings. Write e for the element $(1,0) \in R \times S$. Let M be an $R \times S$ module.

(1) Show that $M = eM \oplus (1-e)M$.
(2) Show how to equip eM with the structure of an R-module, and $(1-e)M$ with the structure of an S-module, so that $M \cong eM \times (1-e)M$ (in the sense of Problem 6.3 .)

Worksheet 7: Comaximal Ideals

We now introduce the notion of comaximal ideals. As we will see, ideals being comaximal is something like integers being relatively prime.

Definition: Suppose R is a commutative ring. Ideals A, B of R are said to be ***comaximal*** provided that $A + B = R$.

Problem 7.1. Show that A and B are comaximal if and only if $1 \in A + B$.

Problem 7.2. If $\mathfrak{m}$ is maximal and I is an ideal, show that either $\mathfrak{m}$ and I are comaximal, or else $I \subseteq \mathfrak{m}$.

Problem 7.3. Let R be a commutative ring and let A and B be ideals. Show that the map $R \to R/A \times R/B$, sending r to the ordered pair $(r \bmod A, r \bmod B)$, is surjective if and only if A and B are comaximal.

Definition: Suppose R is a 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.

Problem 7.4. (**This one is a little tricky:**) Suppose that A and B are comaximal ideals in a commutative ring R. Show that $A \cap B = AB$.

Problem 7.5. 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.

We now show that comaximal is a stronger condition than relatively prime, and is the same in $\mathbb{Z}$.

Problem 7.6. Let R be a commutative ring, let a and b in R, and suppose that aR and bR are comaximal. Show that any g which divides both a and b must be a unit.

Problem 7.7. Show that the ideals $xk[x, y]$ and $yk[x, y]$ are **not** comaximal, although the polynomials x and y are relatively prime in $k[x, y]$.

Problem 7.8. Let a and b be relatively prime integers. Show that the ideals $a\mathbb{Z}$ and $b\mathbb{Z}$ are comaximal.

WORKSHEET 8: THE CHINESE REMAINDER THEOREM

"*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)

A lot of results today are quick citations to past worksheets! Have them ready!

Problem 8.1. Let R be a commutative ring and let A and B be ideals. Describe the "obvious" map $R \to R/A \times R/B$ and show that its kernel is $A \cap B$.

Problem 8.2. Show that, if R is a commutative ring and A and B are comaximal ideals, then $R/AB \cong R/A \times R/B$.

Problem 8.3. (**The Chinese Remainder Theorem**) Show that, if $I_1, I_2, \ldots, I_k$ are a list of pairwise comaximal ideals, then

$$R/\left(I_1 I_2 \cdots I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

Problem 8.4. Show that, if $m_1, m_2, \ldots, m_k$ are a list of pairwise relatively prime integers, then

$$\mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Problem 8.5. Let k be a field and $a_1, a_2, \ldots, a_r$ be distinct elements of k. Show that

$$k[t]/(t-a_1)(t-a_2)\cdots(t-a_r)k[t] \cong k \times \cdots \times k$$

where the right hand side has r factors.

WORKSHEET 9: SIMPLE MODULES

Definition: Let R be a ring and let S be a (left) R-module. The module S is called ***simple*** if $S \neq 0$ and the only R-submodules of S are (0) and S.

Problem 9.1. Let R be a ring, let S be a simple R-module, and let M be any R-module.

(1) Let $\alpha : S \to M$ be an R-module homomorphism. Show that α is either injective or 0.
(2) Let $\beta : M \to S$ be an R-module homomorphism. Show that β is either surjective or 0.

Problem 9.2. Let R be a ring and let I be a left ideal. Show that R/I is simple and if and only if there are no left ideals J with $I \subsetneq J \subsetneq R$. Such a left ideal is called a ***maximal left ideal***.

Problem 9.3. If R is a commutative ring, show that this notion of "maximal left ideal" coincides with the notion of "maximal ideal" we have defined before.

Problem 9.4. If the module S is simple, and x is any nonzero element of S, show that $S = Rx$.

Problem 9.5. In any module M, if there is an element x such that $M = Rx$, show that there is a left ideal I of R such that $M \cong R/I$.

Thus, we have shown that the simple R modules are precisely the R-modules of the form R/I for I a maximal left ideal.

Problem 9.6. (**Schur's Lemma**) Let M be a simple R-module. Let $\phi : M \to M$ be an R-module homomorphism. Show that either $\phi = 0$ or else ϕ is invertible.

Schur's Lemma is the first of many results which will relate a property of a module to a property of its endomorphism ring.

WORKSHEET 10: COMPOSITION SERIES

Let R be a ring and let M be an R-module.

Definition: A chain of submodules of M is a sequence $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_\ell = M$. We call ℓ the ***length*** of the chain.

Definition: A ***composition series*** is a chain of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_\ell = M$ such that each quotient module M_i/M_{i-1} is simple. We recall that the zero module is **not** considered simple, so $M_i \neq M_{i+1}$ in a composition series.

Problem 10.1. Suppose that there is a positive integer L such that, for any chain $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$, we have $\ell \leq L$. Show that M has a composition series. (Hint: Consider a chain of maximal length.)

Definition: We say that M has ***finite length*** if M has a composition series.

Problem 10.2. Let M be an R-module which is a finite set. Show that M has finite length.

Problem 10.3. Let k be a field which is contained in R. Suppose that M is finite dimensional as a k-vector space. Show that M has finite length.

The following nonstandard definition will be convenient:

Definition: A ***quasi-composition series*** is a chain of submodules $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_\ell = M$ such that each quotient module M_i/M_{i-1} is either simple or 0.

Problem 10.4. Show that, if M has a quasi-composition series, then M has a composition series.

Problem 10.5. Let $\alpha : A \hookrightarrow B$ be an injective R-module homomorphism, and let $0 = B_0 \subset B_1 \subset \cdots \subset B_b = B$ be a composition series. Show that $\alpha^{-1}(B_0) \subseteq \alpha^{-1}(B_1) \subseteq \cdots \subseteq \alpha^{-1}(B_b)$ is a quasi-composition series.

Problem 10.6. Let $\beta : B \hookrightarrow C$ be an surjective R-module homomorphism, and let $0 = B_0 \subset B_1 \subset \cdots \subset B_b = B$ be a composition series. Show that $\beta(B_0) \subseteq \beta(B_1) \subseteq \cdots \subseteq \beta(B_b)$ is a quasi-composition series.

This, the property of having a composition series passes to submodules and to quotient modules.

Definition: A ***short exact sequence of R-modules*** is three R-modules A, B and C, and two R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$ such that α is injective, β is surjective and $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$. We write it as $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$.

Throughout the worksheet, let R be a ring and let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-modules.

Last time, we saw that, if $B_0 \subset B_1 \subset \cdots \subset B_\ell$ is a composition series for B, then $\alpha^{-1}(B_0) \subseteq \alpha^{-1}(B_1) \subseteq \cdots \subseteq \alpha^{-1}(B_\ell)$ is a quasi-composition series for A and $\beta(B_0) \subseteq \beta(B_1) \subseteq \cdots \subseteq \beta(B_\ell)$ is a quasi-composition series for C. The next problem is probably the most technical one:

Problem 11.1. With notation as above, show that **exactly one of the following things** is true:

(1) Either $\alpha^{-1}(B_{i-1}) = \alpha^{-1}(B_i)$ and $\beta(B_i)/\beta(B_i) \cong B_i/B_{i-1}$
(2) or else $\alpha^{-1}(B_i)/\alpha^{-1}(B_i) \cong B_i/B_{i-1}$ and $\beta(B_{i-1}) = \beta(B_i)$.

We are now ready to begin our attack on the Jordan-Holder theorem. We make the following temporary definitions:

Definition: Let M be an R-module of finite length and let $0 = M_0 \subset M_1 \subset \cdots \subset M_m = M$ be a composition series. Then we define $\ell(M, M_\bullet)$ to be the length m of the composition series $M_\bullet$. For any simple module S, we define $\mathrm{Mult}(S, M, M_\bullet)$ to the number of indices i for which $M_i/M_{i-1} \cong S$.

Theorem (Jordan-Holder): Let M be an R-module of finite length. Suppose that M has two composition series, $0 = M_0 \subset M_1 \subset \cdots \subset M_m = M$ and $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_n = N$. Then $\ell(M, M_\bullet) = \ell(M, M'_\bullet)$ and, for any simple module S, we have $\mathrm{Mult}(S, M, M_\bullet) = \mathrm{Mult}(S, M, M'_\bullet)$.

In other words, Jordan-Holder shows that $\ell(M)$ and $\mathrm{Mult}(S, M)$ are well-defined quantities.

Problem 11.2. Let $B_\bullet$ be a composition series for B. Define $\tilde{A}_i = \alpha^{-1}(B_i)$ and $\tilde{C}_i = \beta(B_i)$, and let $A_\bullet$ and $C_\bullet$ be the composition series obtained from deleting duplicate elements from $\tilde{A}_\bullet$ and $\tilde{C}_\bullet$. Show that $\ell(B, B_\bullet) = \ell(A, A_\bullet) + \ell(C, C_\bullet)$ and that, for any simple module S, we have $\mathrm{Mult}(S, B, B_\bullet) = \mathrm{Mult}(S, A, A_\bullet) + \mathrm{Mult}(S, C, C_\bullet)$.

Problem 11.3. Show that, if the Jordan-Holder theorem holds for A and C, then it holds for B.

Problem 11.4. Show that the Jordan-Holder theorem holds if the module M is simple.

Problem 11.5. Prove the Jordan-Holder theorem. Hint: Induct on $\min\{\ell : M \text{ has a composition series of length } \ell\}$.

Worksheet 12: Noetherian rings

Due to the Jordan-Holder thoerem, finite length modules are very well behaved. They make a great subject for study, but unfortunately, many modules we meet naturally are not finite length.

A weaker condition than “finite length” is “finitely generated”, which many more modules obey. Over a general ring, finitely generated modules can be very tricky. But, over Noetherian[1] rings, they are not so bad:

Let R be a ring. Consider the following conditions on R.

Condition 1(a): Every left ideal I of the ring R is finitely generated.	Condition 2(a): For any chain of left ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of R, we have $I_r = I_{r+1}$ for all sufficiently large r.	Condition 3(a): Given any nonempty collection $\mathcal{X}$ of left ideals of R, there is some $I \in \mathcal{X}$ which is not properly contained in any other $I' \in \mathcal{X}$.
Condition 1(b): Every left R-submodule M of R^n is finitely generated.	Condition 2(b): For any chain of left R-submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ of R^n, we have $M_r = M_{r+1}$ for all sufficiently large r.	Condition 3(b): Given any nonempty collection $\mathcal{X}$ of left R-submodules of R^n, there is some $M \in \mathcal{X}$ which is not properly contained in any other $M' \in \mathcal{X}$.
Condition 1(c): For any finitely generated left R-module S, every left R-submodule M of S is finitely generated.	Condition 2(c): For any finitely generated left R-module S, for any chain of left R-submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ of S, we have $M_r = M_{r+1}$ for all sufficiently large r.	Condition 3(c): For any finitely generated left R-module S, given any nonempty collection $\mathcal{X}$ of left R-submodules of S, there is some $M \in \mathcal{X}$ which is not properly contained in any other $M' \in \mathcal{X}$.

Problem 12.1.
Prove all these definitions are equivalent.[2]

Definition: A ring which obeys these conditions is called ***left Noetherian***. A ring which obeys these conditions with “right” in place of “left” is called ***right Noetherian***. A ring which is left and right Noetherian is called ***Noetherian***.

[1] Named for Emmy Noether, German mathematician 1882-1935, who has a decent case for being the greatest algebraist of all time.

[2] If you don’t assume the Axiom of Choice, then the conditions in each column are still equivalent to each other, and the implications $3(x) \implies 1(x) \implies 2(x)$ still hold, but I don’t know about the reverse implications. However, the use of Choice in showing $2(x) \implies 3(x)$ is very simple.

WORKSHEET 13: UNIQUE FACTORIZATION DOMAINS (UFDS)

Throughout this worksheet, let R be an integral domain.

> **Definition:** Let r be an element of R. We say that r is ***composite*** if r is nonzero and r can be written as a product of two non-units. We say that r is ***irreducible*** if it is neither composite, nor 0, nor a unit.

Thus every element of R is described by precisely one of the adjectives "zero", "unit", "composite", "irreducible".

> **Definition:** Let $p \in R$. We say that p is ***prime*** if pR is a prime ideal and $p \neq 0$.

Problem 13.1. Let p be a non-zero, non-unit. Show that p is prime if and only if, whenever $p|ab$, either $p|a$ or $p|b$.

Problem 13.2. Show that prime elements are irreducible.

Problem 13.3. Let k be a field and let $k[t^2, t^3]$ be the subring of $k[t]$ generated by t^2 and t^3.

(1) Check that t^2 and t^3 are irreducible in $k[t^2, t^3]$.
(2) Show that t^2 and t^3 are not prime in $k[t^2, t^3]$.

Problem 13.4. Consider the subring $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{C}$.

(1) Show that 2, 3 and $1 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Hint: Use the complex absolute value.
(2) Show that 2, 3 and $1 \pm \sqrt{-5}$ are not prime in $\mathbb{Z}[\sqrt{-5}]$. Hint: $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

We want to say that factorizations into prime elements are unique, but factorizations into irreducible elements need not be. In order to do this, we need some vocabulary.

> **Definition:** We define two elements, p and q, of R to be ***associate*** if there is a unit u such that $p = qu$. We define two factorizations $p_1 p_2 \cdots p_m$ and $q_1 q_2 \cdots q_n$ to be ***equivalent*** if $m = n$ and there is a permutation σ in S_n such that p_j is associate to $q_{\sigma(j)}$.

Problem 13.5. Show that any non-zero, non-unit element of R has at most one factorization into **prime** elements, up to equivalence.

Problem 13.6. Give examples, in the rings $k[t^2, t^3]$ and $\mathbb{Z}[\sqrt{-5}]$, of elements with multiple, nonequivalent, factorizations into **irreducible** elements.

> **Definition:** We'll make the following nonstandard definition: We'll say that R ***has factorizations*** if every non-zero, non-unit[1]n R can be written in **at least** one way as a product of irreducibles.

Problem 13.7. Let R have factorizations. Show that the following conditions are equivalent:

(a) All irreducible elements are prime.
(b) Factorizations into irreducibles are unique, up to equivalence.
(c) Every nonzero, nonunit, element has a factorization into prime elements.

> **Definition:** An integral domain which has factorizations and in which the equivalent conditions in Problem 13.7 hold, is called a ***unique factorization domain***, also known as a ***UFD***.

Problem 13.8. Let R be a Noetherian integral domain.

(1) Let r_1, r_2, r_3 ... be a sequence of elements of R such that r_{j+1} divides r_j for all j. Show that, for j sufficiently large, r_j and r_{j+1} are associates.
(2) Show that R has factorizations.

---

[1] Morally, we should consider the product of the empty set to be 1, so 1 has a factorization into a set of irreducibles, namely the empty set. But trying to get this right would be a notational pain, so we'll just refuse to consider factorizations of units.

WORKSHEET 14: PRINCIPAL IDEAL DOMAINS (PIDS)

Definition: Let R be a commutative ring. An ideal I of R is called ***principal*** if $I = rR$ for some $r \in R$.

Problem 14.1. Show that every ideal in $\mathbb{Z}$ is principal. Do **not** assume unique factorization into primes. (Hint: Take the smallest positive element of the ideal.)

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

Problem 14.2. Show that every PID is Noetherian.

Problem 14.3. Let R be a PID. Let u and v be two relatively prime elements of R meaning that, if g divides u and g divides b, then g is a unit. Show that u and v are comaximal, meaning that $uR + vR = R$.

Problem 14.4. Let R be a PID, let p be an irreducible element of R, and let a be any element of R. Show that either p divides a or else p and a are comaximal.

Problem 14.5. Show that, in a PID, irreducible elements are prime.

Problem 14.6. Show that a PID is a UFD.[1]

We note in particular that we have now shown $\mathbb{Z}$ is a UFD.

Problem 14.7. Since PID's are UFD's, we can talk about GCD's in them. Show that, if R is a PID and a and $b \in R$, then $aR + bR = \mathrm{GCD}(a, b)R$.

Problem 14.8. Suppose R is a PID. Show that every nonzero prime ideal in R is a maximal ideal.

We conclude with some fun and useful lemmas about matrices over PID's:

Problem 14.9. Let R be a PID and let x and $y \in R$. Show that there is a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with entries in R and determinant 1 and
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \mathrm{GCD}(x, y) \\ 0 \end{bmatrix}.$$

Problem 14.10. Let R be a PID and let x and $y \in R$. Show that there are 2×2 matrices U and V with entries in R and determinant 1 such that:
$$U \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} V = \begin{bmatrix} \mathrm{GCD}(x, y) & 0 \\ 0 & \mathrm{LCM}(x, y) \end{bmatrix}.$$
Here $\mathrm{LCM}(x, y) := \frac{xy}{\mathrm{GCD}(x,y)}$.

[1] This need not hold without Choice; Hodges, "Lauchli's algebraic closure of Q", *Proceedings of the Cambridge Philosophical Society*, 1976 showed that it is consistent with ZF for there to be a PID in which some elements have no factorization into irreducibles.

WORKSHEET 15: THE EUCLIDEAN ALGORITHM

To find the greatest common measure of two numbers… (Euclid, *The Elements*, Book VII, Proposition 2)

Starting with two positive integers x_0 and x_1, the Euclidean algorithm[1] recursively defines two sequences of integers x_0, x_1, x_2, … and a_1, a_2, a_3, … as follows: For $n \geq 2$, we have

$$x_n = x_{n-2} - a_{n-1}x_{n-1}$$

with $0 \leq x_n < x_{n-1}$. The algorithm terminates when $x_n = 0$.

Problem 15.1. Compute the sequences x_n and a_n with $x_0 = 321$ and $x_1 = 123$.

Problem 15.2. Show that $\mathrm{GCD}(x_0, x_1) = \mathrm{GCD}(x_1, x_2) = \cdots = \mathrm{GCD}(x_{n-1}, x_n) = x_{n-1}$, where $x_n = 0$.

Let this common GCD be g.

Problem 15.3. Show that there is an elementary matrix E with $E \left[\begin{smallmatrix} x_{n-2} \\ x_{n-1} \end{smallmatrix}\right] = \left[\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right]$. Recall that a 2×2 elementary matrix is one of the form $\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right]$.

Problem 15.4. Show that there is a product of elementary matrices F, with $F \left[\begin{smallmatrix} x_0 \\ x_1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} g \\ 0 \end{smallmatrix}\right]$. (Hint: Remember Problem Set 1?)

Problem 15.5. Show that there exist sequences b_k and c_k such that $b_k x_k + c_k x_{k+1} = g$ and show how to compute the b's and c's using the a's.

Problem 15.6. Demonstrate that your method works by finding b and c such that $b \cdot 321 + c \cdot 123 = 3$.

[1] First recorded by Euclid, a Greek mathematician who lived in roughly 300 BCE.

WORKSHEET 16: EUCLIDEAN RINGS

Definition: Suppose R is an integral domain. A ***norm*** on R is any function $N\colon R \to \mathbb{Z}_{\geq 0}$. The function N is said to be a ***positive norm*** provided that $N(r) > 0$ for all nonzero r. We call N a ***multiplicative norm*** if $N(ab) = N(a)N(b)$.

Some examples: The normal absolute value on $\mathbb{Z}$ is a positive norm. The norm map $N(a+bi) = a^2 + b^2$ on the Gaussian Integers $\mathbb{Z}[i]$ is a positive norm. If k is a field, then we can define a norm on $k[x]$ by $N(p(x)) = \deg p$ for $p \neq 0$ and $N(0) = 0$. [1] We can be a bit more clever and make our norm positive and multiplicative by choosing some positive integer $c \geq 2$ and defining $N(p) = c^{\deg(p)}$ for $p \neq 0$ and $N(0) = 0$.

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, and $r \in R$ with

$$a = bq + r \text{ and } N(r) < N(b).$$

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

Problem 16.1. Let k be a field. Show that k is Euclidean with respect to the norm that $N(0) = 0$ and $N(x) = 1$ for $x \neq 0$.

Problem 16.2. Let k be a field. Verify that $k[x]$ is Euclidean with respect to the norm $N(p) = c^{\deg(p)}$ discussed at the end of the paragraph above.

Problem 16.3. Let R be an integral domain with positive multiplicative norm N, and let K be its field of fractions. For $\frac{a}{b} \in K$, define $N_K\left(\frac{a}{b}\right) = \frac{N(a)}{N(b)}$.

(1) Show that $N_K(\ )$ is a well defined function $K \to \mathbb{Q}_{\geq 0}$.
(2) Show that R is Euclidean with respect to N if and only if, for each $x \in K$, there is an $q \in R$ with $N_K(x - q) < 1$.

Problem 16.4. Verify that $\mathbb{Z}[i]$ is Euclidean with respect to the norm $N(a + bi) = a^2 + b^2$.

Problem 16.5. Show that every Euclidean domain is a PID.

Here are some bonus fun problems about Euclidean domains.

Problem 16.6. Show that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean, with respect to the norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$.

Problem 16.7. Show that $\mathbb{Z}[\sqrt{-3}]$ is **not** Euclidean, with respect to the norm $N(a+b\sqrt{-3}) = a^2+3b^2$, but that $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is Euclidean with respect to the norm $N\left(\frac{c+d\sqrt{-3}}{2}\right) = \frac{c^2+3d^2}{4}$.

Problem 16.8. Let p be a positive prime integer.

(1) Show that $\mathbb{Z}[i]$ has an ideal π with $\#(\mathbb{Z}[i]/\pi) = p$ if and only if there is a square root of -1 in $\mathbb{Z}/p\mathbb{Z}$.
(2) Show that $\mathbb{Z}[i]$ has a principal ideal $(a + bi)\mathbb{Z}[i]$ with $\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$ if and only if p is of the form $a^2 + b^2$.
(3) Conclude the following statement which never mentions the ring $\mathbb{Z}[i]$: A prime p is of the form $a^2 + b^2$ if and only if there is a square root of -1 in $\mathbb{Z}/p\mathbb{Z}$.[2]

Problem 16.9. Let R be a Euclidean domain. Show that there is some nonunit f such that every nonzero residue class in R/fR is represented by a unit of R. Deduce that $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is not Euclidean for any norm function.

[1] Under various circumstances, it can be reasonable to define the degree of the 0 polynomial to be $-\infty$, 0 or ∞. We do not take a stand on this issue here. Some people define the degree of the 0 polynomial to be -1, but David Speyer sees no justification for this.

[2] The primes p for which this occurs are precisely 2 and the primes which are $1 \bmod 4$. Here is a quick proof: If $p \equiv 1 \bmod 4$, then $-1 \equiv (p-1)! \equiv (-1)^{(p-1)/2}((p-1)/2)!^2 \equiv ((p-1)/2)!^2 \bmod p$. Conversely, if p is odd and $-1 \equiv x^2 \bmod p$ then $(-1)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \bmod p$, so $p \equiv 1 \bmod 4$.

WORKSHEET 17: INTRODUCTION TO SMITH NORMAL FORM

The Smith normal form theorem says the following:

Theorem:(Smith Normal Form) Let R be a principal ideal domain and let X be an $m \times n$ matrix with entries in R. Then there invertible $m \times m$ and $n \times n$ matrices U and V, and elements $d_1, d_2, \ldots, d_{\min(m,n)}$ of R, such that

$$X = UDV,$$

where D is the $m \times n$ matrix with $D_{jj} = d_j$ and $D_{ij} = 0$ for $i \neq j$. Moreover, we may assume $d_1 | d_2 | \cdots | d_{\min(m,n)}$ and, with this normalization, the d_j are unique up to multiplication by units.

The d_j are called the ***invariant factors*** of X. We first set up some notation:

Problem 17.1. Let R be any ring. Define an relation $\sim$ on $\mathrm{Mat}_{m \times n}(R)$ by $X \sim Y$ if there are invertible $m \times m$ and $n \times n$ matrices U and V with $Y = UXV$. Show that $\sim$ is an equivalence relation.[1]

Problem 17.2. Here is a more abstract perspective on $\sim$: Let X and $Y \in \mathrm{Mat}_{m \times n}(R)$.

(1) Show that $X \sim Y$ if and only if we can choose vertical isomorphisms making the following diagram commute:

$$\begin{tikzcd} R^n \arrow[r, "X"] \arrow[d, "\cong"] & R^m \arrow[d, "\cong"] \\ R^n \arrow[r, "Y"] & R^m \end{tikzcd}$$

(2) Show that, if $X \sim Y$, then the kernels, cokernels and images of X and Y are isomorphic R-modules.

For nonnegative integers m and n and elements $d_1, d_2, \ldots, d_{\min(m,n)}$ of R, we define $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ to be the $m \times n$ matrix D above. Thus, Smith normal form says that every matrix is $\sim$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1 | d_2 | \cdots | d_{\min(m,n)}$ and the d_j are unique up to multiplication by units.

It will be convenient today to know the following formula. The morally right proof of this result will be more natural in a month so you may assume it for now.

Theorem:(The Cauchy-Binet formula). Let R be a commutative ring. Given an $m \times n$ matrix X with entries in R, and subsets $I \subseteq \{1, 2, \ldots, m\}$ and $J \subseteq \{1, 2, \ldots, n\}$ of the same size, define $\Delta_{IJ}(X)$ to be the determinant of the square submatrix of X using rows I and columns J. Let X and Y be $a \times b$ and $b \times c$ matrices with entries in R and let I and K be subsets of $\{1, 2, \ldots, a\}$ and $\{1, 2, \ldots, c\}$ with $|I| = |K| = q$. Then

$$\Delta_{IK}(XY) = \sum_{J \subseteq \{1,2,\ldots,b\},\ |J| = q} \Delta_{IJ}(X) \Delta_{JK}(Y).$$

The next few problems show how to compute invariant factors.

Problem 17.3. Let R be a UFD. Let U, X and V be $m \times m$, $m \times n$ and $n \times n$ matrices with entries in R. Show that the GCD of the $q \times q$ minors of X divides the GCD of the $q \times q$ minors of UXV.

Problem 17.4. Let R be a UFD. Show that, if $X \sim Y$, then the GCD of the $q \times q$ minors of X is equal to the GCD of the $q \times q$ minors of Y.

Problem 17.5. Let R be a UFD. Let X be an $m \times n$ matrix with entries in R. Show that, if $X \sim \mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1 | d_2 | \cdots | d_{\min(m,n)}$, then $d_1 d_2 \cdots d_q$ is the GCD of the $q \times q$ minors of X.

Problem 17.6. Assuming the Smith normal form theorem for $\mathbb{Z}$, compute the invariant factors of the following matrices:

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \qquad \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \qquad \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}.$$

Problem 17.7. If you have gotten this far, go ahead and prove the Cauchy-Binet formula. It can be done by brute force.

[1] The factorization UDV may remind the reader of singular value decomposition. This is not a coincidence; Smith normal form can be thought of as a non-Archimedean version of singular value decomposition.

WORKSHEET 18: PROOF OF THE SMITH NORMAL FORM THEOREM

Most people find the proof of the Smith normal form theorem for Euclidean domains more intuitive than the case of a general PID. When I went to write them out, they actually came out very similar.

Problem 18.1. (Proof of Smith normal form for Euclidean integral domains) Let R be a Euclidean integral domain with positive norm $N(\ )$. Let $X \in \mathrm{Mat}_{m\times n}(R)$. If $X = 0$, the Smith normal form theorem clearly holds for X, so assume otherwise. Let d be an element of smallest norm among all nonzero elements occurring as an entry in a matrix Y with $Y \sim X$. Let Y be a matrix with $Y \sim X$ and $Y_{11} = d$.

(1) Show that d divides Y_{i1} and Y_{1j} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(2) Show that there is a matrix $Z \sim Y$ with $Z_{11} = d$ and $Z_{i1} = Z_{1j} = 0$ for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(3) Show that d divides Z_{ij} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(4) Show that X is $\sim$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.

Problem 18.2. Consequence of the proof of Smith normal form for Euclidean integral domains: Define a stronger equivalence relation $\sim_E$ where $X \sim_E Y$ if $Y = UXV$ where U and V products of elementary matrices.

(1) Trace through your proof and check that you have shown, in a Euclidean integral domain, that every matrix is $\sim_E$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.
(2) Let R be a Euclidean integral domain. Let $\mathrm{SL}_n(R)$ be the group of $n\times n$ matrices with entries in R and determinant 1. Show that $\mathrm{SL}_n(R)$ is generated by elementary matrices.

To do the case of a general PID, you'll need the following old problems:

(14.9) Let x and $y \in R$ Show that there is a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with entries in R such that $ad - bc = 1$ and
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \mathrm{GCD}(x,y) \\ 0 \end{bmatrix}.$$
(14.10) Let x and y be nonzero elements of R. Show that there are invertible 2×2 matrices U and V with
$$U \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} V = \begin{bmatrix} \mathrm{GCD}(x,y) & 0 \\ 0 & \mathrm{LCM}(x,y) \end{bmatrix}.$$
Here $\mathrm{LCM}(x,y) := \frac{xy}{\mathrm{GCD}(x,y)}$.

Problem 18.3.
Let R be a Noetherian ring (such as a PID) and let $\mathcal{D}$ be a nonempty subset of R. Show that there is an element $d \in \mathcal{D}$ which is "minimal with respect to division": More precisely, show that there is an element such that if $d' \in \mathcal{D}$ divides d, then d divides d' as well.

Problem 18.4. (Proof of Smith normal form for PID's) Let R be a PID and let $X \in \mathrm{Mat}_{m\times n}(R)$. Let $\mathcal{D}$ be the set of all entries occurring in any matrix Y with $Y \sim X$. Let d be as in Problem 18.3 for $\mathcal{D}$ and let Y be a matrix with $Y \sim X$ and $Y_{11} = d$.

(1) Show that d divides Y_{i1} and Y_{1j} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(2) Show that there is a matrix $Z \sim Y$ with $Z_{11} = d$ and $Z_{i1} = Z_{1j} = 0$ for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(3) Show that d divides Z_{ij} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(4) Show that X is $\sim$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.

WORKSHEET 19: CLASSIFICATION OF FINITELY GENERATED MODULES OVER A PID

Problem 19.1. Let S be a commutative ring and let M be a finitely generated S-module.

(1) Show that there is a surjection $S^{\oplus m} \twoheadrightarrow M$ for some m.
(2) Suppose that S is Noetherian (for example, every PID is Noetherian). Show that there is a surjection $S^n \twoheadrightarrow \mathrm{Ker}(S^m \to M)$ for some n.
(3) With hypotheses and assumptions as in the previous part, show that there is an $m \times n$ matrix X with $M \cong S^m/XS^n$.

The previous problem shows that every finitely generated S-module is of the form S^m/XS^n for some $m \times n$ matrix X. Now, and **throughout the worksheet, let R be a PID**. We will see how to understand the structure of R^m/XR^n in terms of the Smith normal form of X.

Problem 19.2.
Let $X \in \mathrm{Mat}_{m\times n}(R)$ and let $(d_1, d_2, \ldots, d_{\min(m,n)})$ be the invariant factors of X.

(1) Show that $R^m/XR^n \cong R^{m-\min(m,n)} \oplus \bigoplus_j R/d_jR$.
(2) Show that $\mathrm{Ker}(X) \cong R^{\#\{j:d_j=0\}+n-\min(m,n)}$.

Problem 19.3. (Classification of modules over a PID: Elementary divisor form) Show that every finitely generated R-module M is of the form $\bigoplus R/d_jR$ for some nonunits $d_1, d_2, \ldots, d_k$ in R with $d_1|d_2|\cdots|d_k$.

Problem 19.4. (Classification of modules over a PID: Prime power form) Show that every finitely generated R-module M is of the form $R^{\oplus r} \oplus \bigoplus R/p_j^{e_j}R$ for some nonnegative integer r, some sequence of prime elements p_j and some sequence of positive integers e_j.

Problems 19.3 and 19.4 each give a list of modules such that every finitely generated R-module M is isomorphic to some module in this list. In for this to be a full classification, we now turn to the problem of checking that these lists do not contain two isomorphic modules, so that we have not listed any isomorphism classes more than once. We'll carry this out for the prime power form.

Problem 19.5. Let q be a prime element of R and let M be an R-module.

(1) Show that R/qR is a field and that, for any $k \geq 0$, that $q^kM/q^{k+1}M$ is an R/qR-vector space.
(2) Let $M = R^{\oplus r} \oplus \bigoplus R/p_j^{e_j}R$ as in Problem 19.4. Give a formula for the dimension of $q^kM/q^{k+1}M$ as an R/qR-vector space in terms of the e_j and r.
(3) Suppose that $R^{\oplus r} \oplus \bigoplus R/p_j^{e_j}R \cong R^{\oplus r'} \oplus \bigoplus R/p_j^{e'_j}R$. Show that $r = r'$ and $e_j = e'_j$.

If you have extra time, do the elementary divisors form as well:

Problem 19.6. Let $d_1, d_2, \ldots, d_k$ and $d'_1, d'_2, \ldots, d'_{k'}$ be nonunits of R with $d_1|d_2|\cdots|d_k$ and $d'_1|d'_2|\cdots|d'_{k'}$, such that $\bigoplus R/d_iR \cong \bigoplus R/d'_iR$. Show that $k = k'$ and d_i is associate to d'_i.

WORKSHEET 20: APPLICATIONS OF JORDAN NORMAL FORM AND RATIONAL CANONICAL FORM

The point of this section is to give some examples of problems where knowing Jordan Normal form is useful.

Problem 20.1. Let A be a 5×5 complex matrix with minimal polynomial $X^5 - X^3$.

(1) What is the characteristic polynomial of A^2?
(2) What is the minimal polynomial of A^2?

Problem 20.2. In this problem, we investigate square roots of matrices:

(1) Let $g \in \mathrm{GL}_n(\mathbb{C})$. Show that there is an h in $\mathrm{GL}_n(\mathbb{C})$ with $h^2 = g$.
(2) Show that there is no matrix h in $\mathrm{GL}_2(\mathbb{R})$ with $h^2 = \left[\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right]$.

Problem 20.3. Let k be an algebraically closed field and let A be an $n \times n$ matrix with entries in k. Show that A can be written in the form $D + N$ where D is diagonalizable, N is nilpotent and $DN = ND$. This is called the ***Jordan-Chevalley decomposition*** of A.[1]

Problem 20.4. Let k be an algebraically closed field[2] and let A be an $n \times n$ matrix with entries in k. We define

$$k[A] = \mathrm{Span}_k(1, A, A^2, A^3, A^4, \dots) \subseteq \mathrm{Mat}_{n\times n}(k).$$
$$Z(A) = \{B \in \mathrm{Mat}_{n\times n}(k) : AB = BA\}.$$

(1) Show that $k[A] \subseteq Z(A)$. (I don't recommend Jordan form here.)
(2) Show that the following are equivalent:
    (a) $\dim_k k[A] = n$.
    (b) $\dim_k Z(A) = n$.
    (c) $k[A] = Z(A)$.
    (d) The minimal polynomial of A is the same as the characteristic polynomial of A.
    (e) For each eigenvalue λ of A, there is only one Jordan block of A.

A matrix which obeys the conditions above is called ***regular***.

(3) For any matrix A, show that $\dim k[A] \leq n$.
(4) For any matrix A, show that $\dim Z(A) \geq n$.

Problem 20.5. Let's prove that a real symmetric matrix is diagonalizable!

(1) Let X be an $n \times n$ real matrix and suppose that X is **not** diagonalizable. Prove that there is a two dimensional subspace V of $\mathbb{R}^n$ such that X takes V to itself by a matrix of the form $\left[\begin{smallmatrix} 0 & -c \\ 1 & -b \end{smallmatrix}\right]$ with $b^2 - 4c \leq 0$. (A hint to handle a technical issue: Notice that the matrices $\left[\begin{smallmatrix} \lambda & 0 \\ 1 & \lambda \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & -\lambda^2 \\ 1 & 2\lambda \end{smallmatrix}\right]$ are similar.)
(2) Now suppose that X is symmetric. Let $\cdot$ be the ordinary dot product on $\mathbb{R}^n$. Show that, for any v and $w \in \mathbb{R}^n$, we have $(Xv) \cdot w = v \cdot (Xw)$.
(3) Now suppose that X is symmetric and non-diagonalizable. Let V be the subspace in part (1) and let v, w be a basis for V on which X acts by the matrix $\left[\begin{smallmatrix} 0 & -c \\ 1 & -b \end{smallmatrix}\right]$ with $b^2 - 4c \leq 0$. Show that $w \cdot w + b(v \cdot w) + c(v \cdot v) = 0$.
(4) Deduce a contradiction. Hint: Recall the Cauchy-Schwarz inequality $(v \cdot w)^2 \leq (v \cdot v)(w \cdot w)$.

[1] The Jordan-Chevalley decomposition is unique, but that is a bit hard for a worksheet; it might occur on a problem set.

[2] In fact, this result is true over any field, except that one needs to refer to generalized Jordan form in (3).(d). I thought that might be a bit too hard for the worksheet though.

WORKSHEET 21: UNIQUE FACTORIZATION IN POLYNOMIAL RINGS

Let R be an integral domain and let F be its field of fractions. We know that $F[x]$ is a Euclidean Domain, hence a PID (Problem 16.5), hence a UFD (Problem 14.6). Thus, if $p(x) \in R[x]$, then $p(x)$ factors uniquely in $F[x]$. In general, the situation in $R[x]$ can be much more complex:

Problem 21.1. Let $R = \mathbb{R}[t^2, t^3]$ and let F be the fraction field of R. Show that the polynomial $x^2 - t^2$ factors in $F[x]$, but is irreducible in $R[x]$.

Problem 21.2. Let $R = \mathbb{R}[t^2, t^3]$ and let F be the fraction field of R. Give two different irreducible factorizations of the polynomial $x^6 - t^6$ over $R[x]$.

As the rest of this worksheet will show, if R is a UFD, then life is much nicer. For the rest of this worksheet:

$$\boxed{\textbf{Assume that } R \textbf{ is a UFD.}}$$

Problem 21.3. Let $p \in R$ be a prime element. Let $a(x)$ and $b(x)$ be polynomials in $R[x]$. Show that, if $a(x)b(x) \in pR[x]$, then either $a(x) \in pR[x]$ or $b(x) \in pR[x]$.

We define a polynomial $a_n x^n + \cdots + a_1 x + a_0$ in $R[x]$ to be ***primitive*** if $\mathrm{GCD}(a_n, \cdots, a_1, a_0) = 1$.

Problem 21.4. (**Gauss's Lemma**) Let $a(x)b(x) = c(x)$ with $a(x)$, $b(x)$ and $c(x) \in R[x]$. Show that $c(x)$ is primitive if and only if $a(x)$ and $b(x)$ are primitive.

Problem 21.5. Let $a(x)b(x) = c(x)$ with $a(x) \in R[x]$ primitive, $b(x) \in F[x]$ and $c(x) \in R[x]$. Show that $b(x) \in R[x]$.

Problem 21.6. Let $p(x) \in R[x]$. Show that the following are equivalent:

(1) $p(x)$ is prime in $R[x]$.
(2) $p(x)$ is irreducible in $R[x]$.
(3) One of the following two conditions holds:
- $p(x)$ is a constant polynomial whose value is a prime element p of R.
- $p(x)$ is primitive in $R[x]$, and is prime in $F[x]$.

Helpful reminder: R and $F[x]$ are UFD's, so prime and irreducible are synonyms in those two rings.

We are now set to prove:

Problem 21.7. Show that, if R is a UFD, then $R[x]$ is a UFD.

In particular, $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$ are UFD's for any field k and any number of variables.

WORKSHEET 22: SOME PROBLEMS ABOUT EXTERIOR ALGEBRA

Problem 22.1. Let e_1, e_2, e_3 be the standard basis of $\mathbb{R}^3$. Expand

$$(e_1 + e_2 + e_3) \wedge (e_1 + 2e_2 + 3e_3)$$

in the basis $e_1 \wedge e_2$, $e_1 \wedge e_3$, $e_2 \wedge e_3$ of $\mathbb{R}^3$.

Problem 22.2. Let $L : \mathbb{C}^n \to \mathbb{C}^n$ be a linear map with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. What are the eigenvalues of $\bigwedge^2 L$? Of $\bigwedge^k L$?

Problem 22.3. Let $v_1, v_2, \ldots, v_d$ be vectors in a vector space V. Show that $v_1 \wedge v_2 \wedge \cdots \wedge v_d = 0$ if and only if the v_i are linearly dependent.

Problem 22.4. Let V be a vector space over a field k and let $\eta \in \bigwedge^d V$ for $d > 0$.

(1) Let v be a nonzero vector in V. Show that $v \wedge \eta = 0$ if and only if η can be factored as $v \wedge \theta$ for $\theta \in \bigwedge^{d-1} V$.
(2) More generally, let $U = \{v \in V : v \wedge \eta = 0\}$ and let $u_1, u_2, \ldots, u_k$ be a basis of U. Show that η can be factored as $u_1 \wedge u_2 \wedge \cdots \wedge u_k \wedge \psi$ for some $\psi \in \bigwedge^{d-k} V$.

Problem 22.5. Let e_1, e_2, e_3 be the standard basis of $\mathbb{R}^3$.

(1) Show that there is a unique isomorphism $h : \bigwedge^2 \mathbb{R}^3 \to \mathbb{R}^3$ such that, for $v \in \mathbb{R}^3$ and $\eta \in \bigwedge^2 \mathbb{R}^3$, we have $v \wedge \eta = (v \cdot h(\eta)) e_1 \wedge e_2 \wedge e_3$. Here the $\cdot$ is the standard dot product.
(2) The ***cross product*** map $V \times V \to V$ is defined by $v \times w := h(v \wedge w)$. Check that this is the cross product you already know.
(3) Let $g \in \mathrm{SO}(3)$. Show that $gh(\eta) = h(\bigwedge^2(g)\eta)$ and show that $g(u \times v) = g(u) \times g(v)$.

Problem 22.6. Let V be a vector space of dimension n. Let $L : V \to V$ be a linear map; we will also write L for the matrix of L. Recall that the adjugate matrix, $\mathrm{Adj}(L)$, is the matrix whose (i, j) entry is $(-1)^{i+j}$ times the determinant of the $(n-1) \times (n-1)$ minor of L where we delete row j and column i. For example,

$$\mathrm{Adj} \begin{bmatrix} r & s & t \\ u & v & w \\ x & y & z \end{bmatrix} = \begin{bmatrix} vz - wy & -(sz - ty) & sw - tv \\ -(uz - wx) & rz - tx & -(rw - tu) \\ uy - vx & -(ry - sx) & rv - su \end{bmatrix}.$$

(1) What is the relation between $\mathrm{Adj}(L)$ and $\bigwedge^{n-1}(L)$?
(2) For any $v \in V$ and $\eta \in \bigwedge^{n-1}(V)$, show that $L(v) \wedge \bigwedge^{n-1}(L)(\eta) = (\det L)(v \wedge \eta)$.
(3) Show that $L\,\mathrm{Adj}(L) = (\det L)\mathrm{Id}_n$.

Worksheet A: Summary of major results

This is a chance to go back through the last several worksheets and track down what you've done. **Throughout, let R be an integral domain.** I would recommend first tracking does all the implications which do hold and only then talk about counterexamples to check that other implications don't.

Problem A.1. Draw arrows indicating which implications exist between the following concepts:

R is a PID	R is Euclidean
R is Noetherian	R is a UFD

Problem A.2. Let I be a nonzero ideal of R. Draw arrows indicating which implications exist between the following concepts:

I is prime	I is maximal
I is of the form (f) for f irreducible	I is of the form (f) for f prime

Problem A.3. Suppose that R is a UFD and let I be a nonzero ideal of R. Draw arrows indicating which implications exist between the following concepts:

I is prime	I is maximal
I is of the form (f) for f irreducible	I is of the form (f) for f prime

Problem A.4. Suppose that R is a PID and let I be a nonzero ideal of R. Draw arrows indicating which implications exist between the following concepts:

I is prime	I is maximal
I is of the form (f) for f irreducible	I is of the form (f) for f prime

WORKSHEET B: RATIONAL CANONICAL FORM OF A MATRIX

Problem B.1. Let k be a field. Make sure everyone in your group remembers how to do the old homework problem: Give an equivalence between (1) $k[t]$-modules which are finite dimensional as k-vector spaces and (2) pairs (V, T) where V is a finite dimensional k-vector space and $T : V \to V$ is a k-linear map.

Problem B.2. Let k be a field and let M_1 and M_2 be $k[t]$-modules which are finite dimensional as k-vector spaces, corresponding to (V_1, T_1) and (V_2, T_2). What is the pair corresponding to $M_1 \oplus M_2$?

Let k be a field and let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0$ be a monic polynomial with coefficients in k. We define the ***companion matrix*** of f by

$$\mathcal{C}(f) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & 0 & \cdots & 0 & -f_2 \\ 0 & 0 & 1 & \cdots & 0 & -f_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -f_{d-1} \end{bmatrix}$$

Problem B.3. Show that $k[x]/f(x)k[x]$ corresponds to the pair $(k^d, \mathcal{C}(f))$.

An $n \times n$ matrix with entries in k is said to be in ***rational***[1] ***canonical form*** if it is a block matrix of the form

$$\begin{bmatrix} \boxed{\mathcal{C}(f_1)} & & & \\ & \boxed{\mathcal{C}(f_2)} & & \\ & & \ddots & \\ & & & \boxed{\mathcal{C}(f_k)} \end{bmatrix}$$

for some monic polynomials $f_1(x)$, $f_2(x)$, …, $f_k(x)$ with $f_1 | f_2 | \cdots | f_k$.

Problem B.4. (**The rational canonical form theorem**) Let V be a finite dimensional k-vector space and let $T : V \to V$ be a k-linear map. Show that there is a basis of V in which T is given by a matrix in rational canonical form, and that the polynomials f_1, f_2, …, f_k are uniquely determined by (V, T).

Problem B.5. Describe the characteristic polynomial of T in terms of f_1, f_2, …, f_k.

Problem B.6. The ***minimal polynomial*** of T is the monic polynomial $g(t) \in k[t]$ of lowest degree such that $g(T) = 0$. Describe the minimal polynomial of T in terms of f_1, f_2, …, f_k.

[1] The word "rational" is because we can put matrices into rational canonical form while staying in the same ground field, unlike Jordan-canonical form where need to pass to a larger field. It does not indicate that the notion is special to the field $\mathbb{Q}$.

WORKSHEET C: JORDAN AND GENERALIZED JORDAN FORM OF A MATRIX

Let λ be an element of k. We[1] define the ***Jordan block*** by

$$J_n(\lambda) = \begin{bmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda \end{bmatrix}$$

Problem C.1. Show that $(x-\lambda)^{n-1}, (x-\lambda)^{n-2}, \ldots, (x-\lambda), 1$ is a basis for $k[x]/(x-\lambda)^n k[x]$ and show that multiplication by x, in this basis, is given by the matrix $J_n(\lambda)$.

A matrix is said to be in ***Jordan normal form*** if it is a block matrix whose blocks are Jordan blocks.

Problem C.2. (**The Jordan normal form theorem**) Suppose that the field k is algebraically closed. Show that each $n \times n$ matrix with entries in k is similar to a matrix in Jordan normal form, and that the Jordan normal form is unique up to reordering blocks.

Let $f = x^d + f_{d-1}x^{d-1} + \cdots + f_1 + 0$ be a monic polynomial with coefficients in k. Let U_d be the $d \times d$ matrix with a 1 in the upper-right corner and all other entries 0. Define the ***generalized Jordan block*** $J_n(f(x))$ to be the $(dn) \times (dn)$ block matrix

$$J_n(f) = \begin{bmatrix} \mathcal{C}(f) & 0 & 0 & \cdots & 0 \\ U_d & \mathcal{C}(f) & 0 & \cdots & 0 \\ 0 & U_d & \mathcal{C}(f) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & U_d & \mathcal{C}(f) \end{bmatrix}$$

Problem C.3. Show that $\{x^i f(x)^j : 0 \leq i < d,\ 0 \leq j < n\}$ is a basis for $k[x]/f(x)^n k[x]$.

Problem C.4. Show that multiplication by x in the above basis is given by the matrix $J_n(f(x))$.

Define a matrix to be in ***generalized Jordan normal form*** if it is a block diagonal matrix where each block is of the form $J_{n_i}(p_i(x))$ and the polynomials $p_i(x)$ are irreducible.

Problem C.5. Show that each $n \times n$ matrix with entries in k is similar to a matrix in generalized Jordan normal form, and that the generalized Jordan normal form is unique up to reordering blocks.

[1] The more standard choice is to take $J_n(\lambda)$ to be the transpose of this. The choice given here is more compatible with the standard choices used to define rational canonical form, so we will adopt it. There is no important difference between these conventions.

Worksheet D: Tensor products of vector spaces

"*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 fuck's sake!*"
"What tensor products taught me about living my life" (Cathy O'Neil),
`https://mathbabe.org/2011/07/20/what-tensor-products-taught-me-about-living-my-life/`

Let k be a field and let V and W be k-vector spaces. Define $V \otimes W$ to be the k-vector space generated by symbols $v \otimes w$, for $v \in V$ and $w \in W$, modulo the following relations:

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2 \quad (v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \quad c(v \otimes w) = (cv) \otimes w = v \otimes (cw) \quad (*).$$

Here v, v_1, $v_2 \in V$, w, w_1, $w_2 \in W$ and $c \in k$.

Problem D.1. Show that $0 \otimes w = v \otimes 0 = 0$.

Problem D.2. Prove the ***universal property of tensor products***: For any vector space k, and any k-bilinear pairing $\langle \, , \, \rangle : V \times W \to X$, there is a unique k-linear map $\lambda : V \otimes W \to X$ such that $\langle v, w \rangle = \lambda(v \otimes w)$.

"*[A]ll the proofs I came up with involved the universal property of tensor products, never the elements themselves. It was incredibly unsatisfying, it was like I could only describe the outside of an alien world instead of getting to know its inhabitants.*" – ibid.

Problem D.3. Let V_1, V_2, W_1, W_2 be k-vector spaces and $\alpha : V_1 \to V_2$ and $\beta : W_1 \to W_2$ be k-linear maps. Show that there is a unique linear map $\alpha \otimes \beta : V_1 \otimes W_1 \to V_2 \otimes W_2$ such that $(\alpha \otimes \beta)(v \otimes w) = \alpha(v) \otimes \beta(w)$.

Problem D.4. Let V_1, V_2, V_3, W_1, W_2, W_3 be k-vector spaces and $\alpha_1 : V_1 \to V_2$, $\alpha_2 : V_2 \to V_3$, $\beta_1 : W_1 \to W_2$ and $\beta_2 : W_2 \to W_3$ be k-linear maps. Show that $(\alpha_2 \otimes \beta_2) \circ (\alpha_1 \otimes \beta_1) = (\alpha_2 \circ \alpha_1) \otimes (\beta_2 \circ \beta_1)$.

At this point, we have the basic formal properties to work with tensor products, but we have almost no ability to compute with them. For example, we don't even know a basis for $k^m \otimes k^n$! We turn to this issue next.

Problem D.5. Let I be a set of vectors spanning V and let J be a set of vectors spanning W. Show that the tensor products $v \otimes w$, for $v \in I$ and $w \in J$, span $V \otimes W$.

Problem D.6. Let U be a vector space and let I be a linearly independent subset of U. Prove that there is a basis B of U containing I. This will require Zorn's Lemma. [1]

Problem D.7. Let U be a vector space, let I be a linearly independent subset of U and let $u \in I$. Show that there is a linear form $\alpha : U \to k$ such that $\alpha(u) = 1$ and $\alpha(u') = 0$ for $u' \in I \setminus \{u\}$.

Problem D.8. Let I be a linearly independent subset of V and let J be a linearly independent subset of W. Show that the tensor products $v \otimes w$, for $v \in I$ and $w \in J$, are linearly independent in $V \otimes W$.

Problem D.9. Let I be a basis of V and let J be a basis of W. Show that the tensor products $v \otimes w$, for $v \in I$ and $w \in J$, are a basis of $V \otimes W$.

That was a lot of abstraction, so let's do something concrete.

Problem D.10.
Let α and β be the linear maps $\mathbb{R}^2 \to \mathbb{R}^2$ given by the matrices $\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. Choose a basis for $\mathbb{R}^2 \otimes \mathbb{R}^2$ and write down the matrix of $\alpha \otimes \beta$.

"*After a few months, though, I realized something. I hadn't gotten any better at understanding tensor products, but I was getting used to not understanding them. It was pretty amazing. I no longer felt anguished when tensor products came up; I was instead almost amused by their cunning ways.*" – ibid.

[1] Although Problems D.6 and D.7 genuinely use the Axiom of Choice, Problems D.8 and D.9 are true without it. Here is a sketch of a proof. Note that the arguments suggested in this worksheet work fine in finite dimensional vector spaces. Now, let V and W be vector spaces of any dimension, let I and J be linearly independent subsets of V and W and suppose for the sake of contradiction that there is a linear relation $\sum c_{vw} v \otimes w$ between elements $v \otimes w$ as above. Note that this linear relation involves only *finitely* many elements of I and J. Moreover, the deduction of this dependence from the relations $(*)$ must also use only finitely many elements of V and W. Let $\overline{V}$ and $\overline{W}$ be the subspaces of V and W spanned by these finitely many elements. Then we obtain a counterexample to Problem D.8 inside $\overline{V} \otimes \overline{W}$, and we have $\dim \overline{V}, \dim \overline{W} < \infty$.

WORKSHEET E: TENSOR ALGEBRAS, SYMMETRIC AND EXTERIOR ALGEBRAS

Let k be a field and let V be a vector space over k. There is a natural isomorphism $(V \otimes V) \otimes V \cong V \otimes (V \otimes V)$ and similarly for higher tensor powers. We therefore write $V^{\otimes n}$ for the n-fold tensor product of V with itself and write elements of $V^{\otimes n}$ as $\sum c_{j_1 j_2 \cdots j_n} v_{j_1} \otimes v_{j_2} \otimes \cdots \otimes v_{j_n}$ without parentheses. We define $V^{\otimes 0}$ to be k.

We define the ***tensor algebra*** $T(V)$ to be $\bigoplus_d V^{\otimes d}$.

Problem E.1. Show that $T(V)$ has a unique ring structure where the product of $\sigma \in V^{\otimes s}$ and $\tau \in V^{\otimes t}$ is $\sigma \otimes \tau \in V^{\otimes (s+t)}$.

Problem E.2.
Let $L : V \to W$ be a linear map. Show that there is a unique map of rings $T(L) : T(V) \to T(W)$ with $T(L)(v) = L(v)$ for $v \in V$.

We define the symmetric algebra $\mathrm{Sym}^\bullet(V)$ to be the quotient of $T(V)$ by the 2-sided ideal generated by all tensors of the form $v \otimes w - w \otimes v$.

Problem E.3. Show that $\mathrm{Sym}^\bullet(V)$ is a commutative ring.

Problem E.4. Show that $\mathrm{Sym}^\bullet(V)$ breaks up as a direct sum $\bigoplus_{d=0}^{\infty} \mathrm{Sym}^d(V)$ where $\mathrm{Sym}^d(V)$ is a quotient of $V^{\otimes d}$.

Problem E.5. Let $x_1, x_2, \ldots, x_n$ be a basis of V. Show that $\{x_{i_1} x_{i_2} \cdots x_{i_d} \ : \ 1 \leq i_1 \leq i_2 \leq \cdots \leq i_d \leq n\}$ is a basis of $\mathrm{Sym}^d(V)$. Show that $\mathrm{Sym}^\bullet(V) \cong k[x_1, \ldots, x_n]$.

We define the exterior algebra, $\bigwedge^\bullet(V)$ to be the quotient of $T(V)$ by the two sided ideal generated by $v \otimes v$ for all $v \in V$. The multiplication in $\bigwedge^\bullet(V)$ is generally denoted $\wedge$.

Problem E.6. Show that, for v and $w \in V$, we have $v \wedge w = -w \wedge v$.

Problem E.7. Show that $\bigwedge^\bullet(V)$ breaks up as a direct sum $\bigoplus_{d=0}^{\infty} \bigwedge^d(V)$ where $\bigwedge^d(V)$ is a quotient of $V^{\otimes d}$.

Problem E.8. Let $e_1, e_2, \ldots, e_n$ be a basis of V. Show that $\{e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_d} \ : \ 1 \leq i_1 < i_2 < \cdots < i_d \leq n\}$ is a basis of $\bigwedge^d(V)$.

Problem E.9. Let $v_1, v_2, \ldots, v_d \in V$. Show that $v_1 \wedge v_2 \wedge \cdots \wedge v_d = 0$ if and only if $v_1, v_2, \ldots, v_d$ are linearly dependent.

We now consider the effect of these constructions on linear maps. Let V and W be k-vector spaces and $L : V \to W$ a linear map.

Problem E.10. Show that there are unique ring maps $\mathrm{Sym}^\bullet(L) : \mathrm{Sym}^\bullet(V) \to \mathrm{Sym}^\bullet(W)$ and $\bigwedge^\bullet(L) : \bigwedge^\bullet(V) \to \bigwedge^\bullet(W)$ with $\mathrm{Sym}^\bullet(L)(v) = L(v)$ and $\bigwedge^\bullet(L)(v) = L(v)$ for $v \in V$.

Problem E.11. Let $L : k^3 \to k^3$ be given by the matrix $\left[\begin{smallmatrix} r & s & t \\ u & v & w \\ x & y & z \end{smallmatrix}\right]$. Compute the matrix of $\bigwedge^2(L) : \bigwedge^2(k^3) \to \bigwedge^2(k^3)$.

Problem E.12. Let $L : k^2 \to k^2$ be given by the matrix $\left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right]$. Compute the matrix of $\mathrm{Sym}^2(L) : \mathrm{Sym}^2(k^2) \to \mathrm{Sym}^2(k^2)$.

Problem E.13. Show that $\bigwedge^d(L \circ M) = \bigwedge^d(L) \circ \bigwedge^d(M)$ and $\mathrm{Sym}^d(L \circ M) = \mathrm{Sym}^d(L) \circ \mathrm{Sym}^d(M)$.

Given an $m \times n$ matrix X with entries in k, and subsets $I \subseteq \{1, 2, \ldots, m\}$ and $J \subseteq \{1, 2, \ldots, n\}$ of the same size, define $\Delta_{IJ}(X)$ to be the determinant of the square submatrix of X using rows I and columns J.

Problem E.14. Prove the Cauchy-Binet formula: Let X and Y be $a \times b$ and $b \times c$ matrices with entries in k and let I and K be subsets of $\{1, 2, \ldots, a\}$ and $\{1, 2, \ldots, c\}$ with $|I| = |J| = q$. Then

$$\Delta_{IK}(XY) = \sum_{\substack{J \subseteq \{1, 2, \ldots, b\} \\ |J| = q}} \Delta_{IJ}(X) \Delta_{JK}(Y).$$

Worksheet F: Bilinear forms

Suppose k is a field and V is a k-vector space.

Definition. A *k-bilinear form on V* is a bilinear pairing $B : V \times V \to k$. A k-bilinear form B is said to be

- ***symmetric*** provided that $B(x, y) = B(y, x)$ for all x and $y \in V$,
- ***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 and $t \in V$.

Problem F.1. Show that every alternating form is skew symmetric. Hint for this problem and the next two: Think about $B(v + w, v + w)$.

Problem F.2. Show that, if the characteristic of k is not 2, then every skew-symmetric form is alternating.

Problem F.3. Show that, if the characteristic of k is not 2 and B is a symmetric bilinear form with $B(v, v) = 0$ for all $v \in V$, then $B(v, w) = 0$ for all v and $w \in V$.

We now restrict our attention to the finite dimensional case: Let $v_1, v_2, \dots, v_n$ be a basis of V and let G be the $n \times n$ matrix $G_{ij} = B(v_i, v_j)$. We call G the ***Gram matrix***.[1]

Problem F.4. In the basis $v_1, \dots, v_n$, verify the formula $B(\vec{x}, \vec{y}) = \vec{x}^T G\vec{y}$.
Under what conditions on G will B be symmetric?
Under what conditions on G will B be alternating?
Under what conditions on G will B be skew-symmetric?

Problem F.5. Let $w_1, w_2, \dots, w_n$ be a second basis of V, with $w_j = \sum S_{ij} v_i$. Let H be the Gram matrix $B(w_i, w_j)$. Give a formula for H in terms of S and G.

A bilinear form B on V is called ***nondegenerate*** if, for all $v \in V$, there is some $w \in V$ with $B(v, w) \neq 0$.

Problem F.6. Let V be a finite dimensional vector space. Show that B is nondegenerate if and only if the Gram matrix of B is invertible.

Problem F.7. Let V be a finite dimensional[2] vector space, let B be a bilinear form on V and let L be a subspace of V such that the restriction of B to L is nondegenerate. Define $L^\perp = \{v \in V : B(u, v) = 0 \ \forall u \in L\}$. Show that $V = L \oplus L^\perp$.

Remark If we are dealing with a general form, we should define both $L^\perp = \{v \in V : B(u, v) = 0 \ \forall u \in L\}$ and ${}^\perp L = \{v \in V : B(v, u) = 0 \ \forall u \in L\}$. Then we have both $V = L \oplus L^\perp$ and $V = L \oplus {}^\perp L$. However, both for symmetric and skew-symmetric forms we have $L^\perp = {}^\perp L$, so we don't need to make this distinction.

[1] The term Gram matrix is generally used in the context of applied linear algebra, such as computer graphics and control theory. In that context, the vector space V is simply $\mathbb{R}^n$ and B is simply dot product, but v_i is some basis of $\mathbb{R}^n$ which is not orthonormal. The Gram matrix encodes the "skewness" of our basis.

[2] Without finite dimensionality, this is not true. Let V be a vector space with basis $e_1, e_2, e_3, \dots$ and consider the standard bilinear form $B\left(\sum a_i e_i, \sum b_i e_i\right) = \sum a_i b_i$. Let L be the subspace spanned by $e_i - e_j$. Then $L^\perp$ is 0 because, if $\sum a_k e_k$ is perpendicular to all $e_i - e_j$ then $a_i = a_j$ for all i, j. But V only allows finite sums, so the only such elements are 0.

WORKSHEET G: SYMMETRIC BILINEAR FORMS

Let k be a field, let V be a finite dimensional vector space over k and let $B : V \times V \to k$ be a k-bilinear pairing. Recall that, given a basis $v_1, v_2, \ldots, v_n$ of V, we encode B in a Gram matrix G with $G_{ij} = B(v_i, v_j)$, and that B is symmetric if and only if G is. Changing bases of V modifies the Gram matrix by $G \mapsto SGS^T$ for invertible S. It is natural to ask how nice we can make the matrix G by action of this kind.

To simplify our results, assume that k does not have characteristic 2.

Problem G.1. Suppose that B is a symmetric bilinear form. Show that there is a basis of V for which the Gram matrix of B is diagonal. (Hint: If $B \neq 0$, use Problem F.3 to find a vector v with $B(v, v) \neq 0$, then consider the decomposition $V = kv \oplus (kv)^{\perp}$.)

Problem G.2. Let G be a symmetric matrix with entries in k. Show that there is an invertible matrix S and a diagonal matrix D such that $G = SDS^T$.

Problem G.3. Let $k = \mathbb{Q}$. Carry out the procedure in the previous problems for

(1) $G = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$.

(2) $G = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}$.

This immediately raises the question, given two diagonal matrices $\mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_n)$, when are the bilinear forms $\vec{x}^T \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)\vec{y}$ and $\vec{x}^T \mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_n)\vec{y}$ equivalent up to a change of basis? For a general field, this is a very hard question. However, we can say some things.

Problem G.4. Suppose that there are nonzero scalars γ_i in k with $\alpha_i = \gamma_i^2 \beta_i$. Show that the $\vec{x}^T \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)\vec{y}$ and $\vec{x}^T \mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_n)\vec{y}$ are equivalent.

Problem G.5. Show that the bilinear forms $B(\left[\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right], \left[\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right]) = x_1x_2 + y_1y_2$ and $C(\left[\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right], \left[\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right]) = 5x_1x_2 + 5y_1y_2$ are related by a change of basis in $\mathbb{Q}^2$, even though 5 is not square in $\mathbb{Q}$.

Problem G.6. Let $k = \mathbb{R}$. Show that any bilinear form over $\mathbb{R}$ can be represented by a diagonal matrix whose entries lie in $\{-1, 0, 1\}$.

WORKSHEET H: SYMMETRIC BILINEAR FORMS OVER $\mathbb{R}$

Let B be a symmetric bilinear form on a vector space W over $\mathbb{R}$. We say that B is

- ***Positive definite*** if $B(w, w) > 0$ for all nonzero $w \in W$.
- ***Positive semidefinite*** if $B(w, w) \geq 0$ for all $w \in W$.
- ***Negative definite*** if $B(w, w) < 0$ for all nonzero $w \in W$.
- ***Negative semidefinite*** if $B(w, w) \leq 0$ for all $w \in W$.

Recall that we showed in Problem G.6 that a symmetric bilinear form over $\mathbb{R}$ can always be represented by a diagonal matrix whose entries lie in $\{-1, 0, 1\}$.

Problem H.1. Let B be a symmetric bilinear form which can be represented by the diagonal matrix

$$\mathrm{diag}(\overbrace{1,1,\ldots,1}^{n_+},\overbrace{0,0,\ldots,0}^{n_0},\overbrace{-1,-1,\ldots,-1}^{n_-}).$$

(1) Show that n_+ is the dimension of the largest subspace L of V such that B restricted to L is positive definite.
(2) Show that $n_+ + n_0$ is the dimension of the largest subspace L of V such that B restricted to L is positive semidefinite.
(3) Show that n_- is the dimension of the largest subspace L of V such that B restricted to L is negative definite.
(4) Show that $n_- + n_0$ is the dimension of the largest subspace L of V such that B restricted to L is negative semidefinite.

Problem H.2. Let B be a symmetric bilinear form. Suppose that B can be represented (in two different bases) by the diagonal matrices

$$\mathrm{diag}(\overbrace{1,1,\ldots,1}^{m_+},\overbrace{0,0,\ldots,0}^{m_0},\overbrace{-1,-1,\ldots,-1}^{m_-}) \text{ and } \mathrm{diag}(\overbrace{1,1,\ldots,1}^{n_+},\overbrace{0,0,\ldots,0}^{n_0},\overbrace{-1,-1,\ldots,-1}^{n_-}).$$

Show that $(m_+, m_0, m_-) = (n_+, n_0, n_-)$.

The word ***signature*** is used to refer to something like the triple (n_+, n_0, n_-). Unfortunately, sources disagree as to exactly what the signature is. Various sources will say that the signature is (n_+, n_0, n_-), (n_+, n_-, n_0), (n_+, n_-) or $n_+ - n_-$. In this course, we'll adopt the convention that the signature is (n_+, n_0, n_-). If G is a symmetric real matrix, we will use the term ***signature of*** G to refer to the signature of the bilinear form $B(x, y) = x^T G y$.

Problem H.3.
Let G be a real symmetric $n \times n$ matrix with signature (n_+, n_0, n_-). If $n_0 > 0$, show that $\det G = 0$. If $n_0 = 0$, show that $\det G$ is nonzero with sign $(-1)^{n_-}$.

Problem H.4. Let G be a real symmetric $n \times n$ matrix with signature (n_+, n_0, n_-). Let G' be the upper left symmetric $(n-1) \times (n-1)$ submatrix of G. Show that the signature of G' is one of $(n_+ - 1, n_0 + 1, n_- - 1)$, $(n_+ - 1, n_0, n_-)$, $(n_+, n_0, n_- - 1)$, $(n_+, n_0 - 1, n_-)$. Hint: Use Problem H.1.

Problem H.5. Let G be a real symmetric matrix and let G_k be the $k \times k$ upper left submatrix of G. Assume that $\det G_k \neq 0$ for $1 \leq k \neq n$. Show that the signature of G is $(n - q, 0, q)$ where q is the number of k for which $\det G_{k-1}$ and $\det G_k$ have opposite signs. Here we formally define $\det G_0 = 1$.

Problem H.6. (**Sylvester's criterion**) Let G be a real symmetric matrix and define G_k as above. Show that G is positive definite if and only if all the $\det G_k$ are > 0. (In other words, we no longer have to take $\det G_k \neq 0$ as an assumption.)