Math 122 Homework Seven

1. Basic ring homomorphisms

(a) Show that any ring homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ must be the identity function.

(b) Show that any ring homomorphism $f : \mathbb{Q} \to \mathbb{Q}$ must be the identity function.

(c) Exhibit a ring homomorphism $f : \mathbb{C} \to \mathbb{C}$ which is not the identity function.

(d) Show that there is no ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$.

2. Really?

Show that the only ring homomorphism from $\mathbb{R}$ to itself is the identity. (This problem is more subtle—and more fun—than it sounds.)

3. Some important rings

(a) Suppose that $0 = 1$ in a ring R. Show that R contains exactly one element. We will call this the *zero ring*.

(b) For any ring R, show that there is a unique ring homomorphism from R to the zero ring. (That is, if f and g are two ring homomorphisms, then $f(x) = g(x)$ for all $x \in R$.)

(c) Show that if a ring R has more than one element, it does not admit a ring homomorphism from the zero ring.

(d) Show that any ring R receives a unique ring homomorphism from $\mathbb{Z}$.

(e) Let $\mathbb{Z}[x]$ denote the polynomial ring where all coefficients are integers. Show that for any ring R, there is a bijection between $\hom_{Ring}(\mathbb{Z}[x], R)$ and R itself.

4. Computing in $\mathbb{Z}/n\mathbb{Z}$

(a) Write out the multiplication table for the ring $\mathbb{Z}/5\mathbb{Z}$.

(b) Write out the multiplication table for the ring $\mathbb{Z}/6\mathbb{Z}$.

(c) Show that the cancellation law fails in $\mathbb{Z}/6\mathbb{Z}$—that is, exhibit an example of a, b, c so that $ac = bc$ but $a \neq b$.

(d) Recall that a *square root of* b is some element a such that $a^2 = b$. Does either of the above two rings contain a square root of -1? Prove your claims for each ring.

5. (Optional) So many variables

For every integer $n \geq 2$, Exhibit a ring R_n so that, for any *commutative* ring S, there is a bijection

$$\hom_{Ring}(R_n, S) \to S^n.$$

Here, S^n is the set of ordered n-tuples $(s_1, \ldots, s_n)$ with $s_i \in S$.

6. (Optional) The quaternion ring

Here, we define a ring structure on $\mathbb{R}^4$. Addition is the usual addition of vectors. To describe multiplication, it's convenient to write an element of $\mathbb{R}^4$ as consisting of a scalar t and a vector $\vec{v}$:

$$(t, \vec{v}) \in \mathbb{R} \times \mathbb{R}^3 \cong \mathbb{R}^4.$$

Then define

$$(s, \vec{u}) \cdot (t, \vec{v}) := (st - \vec{u} \cdot \vec{v}, s\vec{v} + t\vec{u} + \vec{u} \times \vec{v}).$$

We will call this ring the *quaternions*, or the *Hamiltonians*. We denote it by $\mathbb{H}$. (The $\cdot$ and $\times$ are the usual dot and cross products from three-dimensional geometry.)

Sometimes, it is customary to pick out three elements as follows:

$$i = (0, (1, 0, 0)), \qquad j = (0, (0, 1, 0)), \qquad k = (0, (0, 0, 1)).$$

(a) Verify that $\mathbb{H}$ is an associative ring.

(b) Show by example that $\mathbb{H}$ is not commutative.

(c) Verify the following:

$$ij = k, \qquad jk = i, \qquad ik = -j,$$

and

$$i^2 = j^2 = k^2 = -1.$$

(d) Recall that the complex numbers have exactly two square roots of -1. Exhibit a complete list of square roots of -1 in $\mathbb{H}$. Prove your list is complete.

(e) Let $Hom_{Ring}(\mathbb{C}, \mathbb{H})$ be the set of ring homomorphisms from $\mathbb{C}$ to $\mathbb{H}$. Construct an injection from S^2 to $Hom_{Ring}(\mathbb{C}, \mathbb{H})$. Here, S^2 is the set

$$S^2 := \{(x, y, z) \text{ such that } x^2 + y^2 + z^2 = 1\ \} \subset \mathbb{R}^3$$

otherwise known as the sphere.

(f) Recall $\mathbb{H}^\times$ is the group of units of $\mathbb{H}$. Show that $S^3 \subset \mathbb{H}^\times$ is a normal subgroup. Exhibit a group isomorphism from $\mathbb{H}^\times / S^3$ to another group you know.

Math 122 Homework Eight

Due Wed, Nov 1.

Some basic facts for groups

You don't need to prove these, and even if you hand in proofs, we won't grade them—but these are facts that hopefully jive with some of the intuitions you've built up in the last two months. You may assume these facts from now on, and should prove them if you feel like it. (Many of you have proven variations in your homework.) I'm listing these here as a collective reference of the class.

(a) Fix an integer $n \geq 1$ and let $Ord_n(G)$ denote the set of elements in G with order n (it could be empty). If $\phi : G \to H$ is a group isomorphism, ϕ induces a bijection $Ord_n(G) \cong Ord_n(H)$. This also holds when $n = \infty$.

(b) Let *Subgp*(G) denote the set of subgroups of G. Then any group isomorphism $\phi : G \to H$ induces a bijection *Subgp*$(G) \cong$ *Subgp*(H). Likewise, if
   (a) *Subgp*$^{normal}(G)$ denotes the collection of normal subgroups,
   (b) *Subgp*$^{k}(G)$ denotes the collection of all subgroups of order k,
   (c) *Subgp*$^{indexk}(G)$ denotes the collection of all subgroups $G' \subset G$ such that $|G/G'| = k$,

then for any value of $* \in \{normal, k, indexk\}$, ϕ induces a bijection

$$Subgp^*(G) \cong Subgp^*(H).$$

(c) If $\phi : G \to H$ and $\psi : H \to I$ are group homomorphisms, so is the composition $\psi \circ \phi$.

Okay, onto the problems in the problem set.

1. Actions and modules

(a) Let R be a ring and M an abelian group. Exhibit a bijection between (i) The set of functions $\mu : R \times M \to M$ exhibiting a left R-module structure on M, and (ii) The set of ring homomorphisms $R \to End(M)$. (Hint: For any fixed $r_0 \in R$, show that $\mu(r_0, -)$ is an endomorphism of M.)

(b) Let G be a group and X a set. Exhibit a bijection between (i) The set of functions $\mu : G \times X \to X$ exhibiting a left G-action on X, and (ii) The set of group homomorphisms $G \to Aut_{Set}(X)$. (Hint: For any fixed $g_0 \in G$, show that $\mu(g_0, -)$ is a bijection from X to itself.)

(c) Let $\phi : R \to S$ be a ring homomorphism. Show that the function $R \times S \to S$ given by $(r, s) \mapsto \phi(r)s$ makes S into a left R-module.

(d) Show that any ring R can be given the structure of a left module over itself (i.e., R is an R-module).

(e) Using 3(d) from last homework, show that any abelian group admits a unique $\mathbb{Z}$-module structure.

2. Fields

Recall that a *field* is a ring R satisfying the following: $0 \neq 1$, R is commutative, and every $x \neq 0$ is a unit.

(a) Show that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

(b) Exhibit an example of an ideal in $\mathbb{Z}$ which is prime, but not maximal. Show that, except for your example, all other prime ideals are maximal. (Hint: Think trivially.)

(c) Let $(R, +) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as an abelian group. Come up with a multiplication $\times$ on R so that (i) $(R, +, \times)$ is a field, and (ii) the element $(1, 0) \in R$ is the multiplicative unit. (This second requirement is just to make our grading easier.) In particular, you have exhibited a field with four elements.

3. Can you $\mathbb{C}$?

(a) Let $f(x) = x^2 + 1 \in \mathbb{R}[x]$, and $(f) \subset \mathbb{R}[x]$ the ideal generated by f. Show that the quotient ring $\mathbb{R}[x]/(f)$ is a vector space of dimension two over $\mathbb{R}$. (Hint: Show that any polynomial g is related to a polynomial of degree ≤ 1 under the usual equivalence relation. You should look up long division of polynomials if you haven't seen it before.)

(b) Exhibit a ring isomorphism $\mathbb{R}[x]/(f) \to \mathbb{C}$. Use universal properties.

Let G be the set of ring isomorphisms $\phi : \mathbb{C} \to \mathbb{C}$ such that $\phi(t) = t$ for all $t \in \mathbb{R}$. Put another way, G is the set of automorphisms of $\mathbb{C}$ which fix $\mathbb{R}$.

(c) Show that G is a group under composition.

(d) Show that G is isomorphic to a group we've seen before—which one? Prove it.

By the way, if you take Math 123, G will be written $Gal(\mathbb{C}/\mathbb{R})$. It is the *Galois group* of the field extension $\mathbb{C}/\mathbb{R}$.

4. Polynomials

Let $\mathbf{k}$ be a field and $f \in \mathbf{k}[x]$ a polynomial. Then f is called *irreducible* if there whenever $f = gh$, either g or h is a constant polynomial (i.e., either g or h only has a constant term).

Also: An element $y \in \mathbf{k}$ is called a *root* of f if $f(y) = 0$. Written out, recall that if

$$f = \sum_{i=0}^{d} a_i x^i \in \mathbf{k}[x]$$

then

$$f(y) = \sum_{i=0}^{d} a_i y^i \in \mathbf{k}.$$

We say that f *admits a root* if there is some $y \in \mathbf{k}$ so that $f(y) = 0$.

Throughout this problem, it may be useful to know that $\deg(fg) = \deg(f) + \deg(g)$.

(a) Show that any constant or linear polynomial is irreducible in $\mathbf{k}[x]$ (i.e., any polynomial of degree ≤ 1 is irreducible).

(b) Let $\mathbf{k} = \mathbb{Z}/2\mathbb{Z}$. Write down every irreducible polynomial of degree ≤ 3. (There are many ways to do this; it may help to flip the question and find all the reducible ones first. Alternatively, it's not so hard to add zeroes and ones mod 2.)

(c) Let $\mathbf{k} = \mathbb{Z}/3\mathbb{Z}$. Write down every irreducible polynomial of degree ≤ 2.

5. (Optional) Some simple extras.

For full credit, your solution must be well-written and concise.

(a) Let R and S be finite rings such that neither ring is the zero ring. Show that if $gcd(|R|, |S|) = 1$, then there does not exist any ring homomorphism from R to S, nor from S to R. (Hint: Lagrange.)

(b) Let G and H be groups. Show that if $|H|$ and $|G|$ are finite, then $|G/H|$ is equal to $|G|/|H|$. (We have used this fact before; but you haven't proven it in homework; try orbit-stabilizer.)

6. (Optional) Some simple extras, II.

For full credit, your solution must be well-written and concise.

(a) Let $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ be the set of all elements of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Show that $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

(b) Show that $\mathbb{Q}[\sqrt{2}]$ is a field.

7. (Optional)

Fix an abelian group M, and an integer $n \geq 2$. Show that the following are equivalent:

(a) M admits the structure of a $\mathbb{Z}/n\mathbb{Z}$-module.

(b) M admits the structure of a $\mathbb{Z}/n\mathbb{Z}$-module, and this structure is unique.

(c) Every element of M has order dividing n.

(d) M admits the structure of a $\mathbb{Z}/n\mathbb{Z}$-module, and every *subgroup* of M is automatically a submodule.

(e) Any subgroup of M admits the structure of a $\mathbb{Z}/n\mathbb{Z}$-module.

8. (Optional) Characteristic subgroups

A subgroup $H \subset G$ is called *characteristic* if for any group automorphism $\phi : G \to G$, we have that $\phi(H) = H$.

(a) Show that a characteristic subgroup of G is always a normal subgroup.

(b) Show that the commutator subgroup $[G, G]$ is characteristic. (This shows, in particular, the $[G, G]$ is normal.)

(c) Show that the center is a characteristic subgroup.

Homework Nine

Due Wed, Nov 8.

1. Euclid is making us divisive

In what follows, I give you two polynomials f, g and a field $\mathbf{k}$. Using the algorithm for dividing polynomials, find the unique polynomials $h, r \in \mathbf{k}[x]$ with $\deg r < \deg g$ so that

$$f = hg + r.$$

(a) $f = x^3 + 2$; $g = x + 2$; $\mathbf{k} = \mathbb{Z}/3\mathbb{Z}$.

(b) $f = x^3 + 2$; $g = x + 2$; $\mathbf{k} = \mathbb{Q}$

(c) A polynomial f with coefficients in a field $\mathbf{k}$ is called *irreducible* if whenever $f = gh$, either g or h is a constant polynomial. Show that if $f \in \mathbf{k}[x]$ is an irreducible polynomial and if $\deg f \geq 2$, then f has no roots in $\mathbf{k}$. (I.e., there does not exist any $y \in \mathbf{k}$ so that $f(y) = 0$.)

2. Let's count

Fix a field $\mathbf{k}$. Assume $\mathbf{k}$ is finite, and let $q = |\mathbf{k}|$. (For example, if $\mathbf{k}$ is $\mathbb{Z}/p\mathbb{Z}$ for a prime p, we have $q = p$.)

(a) Let $GL_n(\mathbf{k})$ denote the set of $n \times n$ invertible matrices with entries in $\mathbf{k}$. (Recall that a matrix A is *invertible* if there exists another matrix B such that $AB = BA = I$, where I is the identity matrix.) Show that this is a group in at most four sentences. Make your sentences concise.

(b) Show that $GL_n(\mathbf{k})$ has order

$$\prod_{i=0}^{n-1}(q^n - q^i) = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}).$$

(c) Let $H \subset GL_n(\mathbf{k})$ be the subset consisting of all matrices that are *upper-triangular*, meaning $A \in H$ if and only if for all $j < i$, $A_{ij} = 0$. Show that H is a subgroup. Compute the order of H.

(d) Let $L \subset GL_n(\mathbf{k})$ be the subset consisting of all matrices that are upper-triangular with 1 along the diagonal, meaning $A \in H$ if and only if for all $j < i$, $A_{ij} = 0$ and $A_{ii} = 1$. Show that L is a subgroup. Compute the order of L.

3. (Optional) Characteristic

Let $\mathbf{k}$ be a field. Recall that there is a unique ring homomorphism $\phi : \mathbb{Z} \to \mathbf{k}$. We let n be the positive integer such that the kernel of ϕ is $n\mathbb{Z}$.

(a) If $n \neq 0$, show that n is the smallest positive integer for which $1 + \ldots + 1 = 0$ in $\mathbf{k}$.

(b) Show that n must be a prime number. Thus, to every field $\mathbf{k}$, we've attached a number—either 0, or a prime number p. This is called the *characteristic* of $\mathbf{k}$.

(c) Show that $\mathbb{Z}/p\mathbb{Z}$ has characteristic p, and that $\mathbb{Q}$ has characteristic 0.

(d) Show that if $\mathbf{k}$ admits a ring homomorphism to another field F, then $\mathbf{k}$ and F have the same characteristic.

4. (Optional) Some field stuff.

(a) Let F be a field and R a non-zero ring. Show that any ring homomorphism $\phi : F \to R$ must be an injection.

(b) Show that if F is a finite field, there is some prime p such that $\mathbb{Z}/p\mathbb{Z}$ admits an injective ring homomorphism into F.

(c) Show that if F is a finite field, it can be given the structure of a vector space over $\mathbb{Z}/p\mathbb{Z}$ for some p.

(d) Show that if F is a finite field, it has size p^N for some integer $N \geq 1$.

5. (Optional) The darned square root of -5.

Let $R = \mathbb{Z}[\sqrt{-5}]$ denote the subring of $\mathbb{C}$ consisting of elements of the form

$$a + bi\sqrt{5}, \qquad a, b \in \mathbb{Z}.$$

(a) Show that R is indeed a subring. (I.e., it's a subgroup under $+$, it's closed under $\times$, and it contains 1.)

(b) Let $N(a + bi\sqrt{5}) := a^2 + 5b^2$. Show that for $x, y \in R$, we have $N(x)N(y) = N(xy)$.

(c) Show that you can factor the element $6 \in R$ in two non-equivalent ways. More precisely, show that you can find elements $w, x, y, z \in R$ so that

$$6 = xy = wz$$

where x is not a multiple of w nor of z, and y is not a multiple of w nor of z. This shows that R doesn't have a notion of "prime factorization" like $\mathbb{Z}$ does.

(d) Find all units of R.

Homework 10

Due Wednesday, Nov 15.

1. Irreducibles and primes

Let R be a ring. An element $x \in R$ is called *irreducible* if (i) x is not a unit, and (ii) whenever $x = uv$, at least one of u and v is a unit in R. (So either u or v divides 1.)

Let $\mathbf{k}$ be a field. We say that a polynomial $f(x) \in \mathbf{k}[x]$ is *irreducible* if f is irreducible in the above sense, taking $R = \mathbf{k}[x]$. (Note the modification from a previous homework; the old definition was incorrect—we should demand that f is not a unit.)

(a) Show that the units of $\mathbf{k}[x]$ are precisely the constant, non-zero polynomials.

(b) Show that if f is irreducible and degree $f \geq 2$, then f does not have a root in $\mathbf{k}$. (Hint: If $a \in \mathbf{k}$ is a root, try to divide f by $x - a$.)

(c) Show that f is irreducible, then $(f) \subset \mathbf{k}[x]$ is a prime ideal. You can assume that two elements f, g in $\mathbf{k}[x]$ have a gcd—some polynomial of highest degree dividing both f and g. Moreover, you can assume that if $gcd(f, g) = h$, then there exist $a, b \in \mathbf{k}[x]$ such that $af + bg = h$. This may help in 2(b) as well.

(d) Conversely, suppose that f is non-zero and that (f) is a prime ideal. Show that f is irreducible.

2. Polynomial rings with field coefficients are PIDs

Let $\mathbf{k}$ be a field.

(a) Let $I \subset \mathbf{k}[x]$ be an ideal. Show that $I = (f)$ for some $f \in \mathbf{k}[x]$. (Hint: Let $f(x) \in I$ be a polynomial of least degree in I. Long division is your friend.)

(b) Let I be any non-zero, proper ideal of $\mathbf{k}[x]$. Show that I is prime if and only if I is maximal.

(c) If $f \in \mathbf{k}[x]$ is irreducible, show that $\mathbf{k}[x]/(f)$ is a field.

3. (Optional) Think rationally

(a) Let $(\mathbb{Q}, +)$ be the group of rational numbers under addition. Show this group is not the direct product of two proper subgroups.

(b) Let $G = (\mathbb{Q} - \{0\}, \times)$ be the group of non-zero rational numbers under multiplication. Let $H = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}^{\oplus \mathbb{N}})$, where $\mathbb{Z}^{\oplus \mathbb{N}}$ is the set consisting of sequences of integers that are eventually zero. Equivalently, an element of $\mathbb{Z}^{\oplus \mathbb{N}}$ is a sequence of integers

$$\vec{a} = (a_0, a_1, a_2, \ldots),$$

where $a_i \neq 0$ for only finite many i. We make $\mathbb{Z}^{\oplus \mathbb{N}}$ into a group by component-wise addition.

Prove or disprove: G is isomorphic to H.

4. (Optional) They look so similar... or do they?

Determine which of the following groups are isomorphic to another.

(a) The group $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ of group automorphisms of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(b) The group of invertible 2×2 matrices with entries in the ring $\mathbb{Z}/2\mathbb{Z}$.
(c) The group S_3.
(d) The group D_6 of symmetries of a triangle.
(e) The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

5. (Optional) Order, order!

(a) Exhibit elements of $GL_2(\mathbb{Z})$ of order 1, 2, 3, 4, and 6.

(b) Follow through on the strategy outlined in class to show that there is no element $A \in GL_2(\mathbb{Z})$ of order 5. (Indeed, 1, 2, 3, 4, and 6 are the only possible orders, but we don't quite yet have the math to prove that yet.)

Homework 11

Due Monday, November 27, by 1:50 PM. This week's optionals problems are a lot of fun. Some of these problems require thought, so you should get an early start.

1. Dimension

Let R be a commutative ring. The *Krull dimension*, or *dimension* of R is defined to be the maximum integer $n \geq 0$ such that one can find a collection of prime ideals

$$p_0 \subset p_1 \subset \ldots \subset p_n \subset R.$$

Note that this collection begins with p_0, not p_1, and that each inclusion $p_i \subset p_{i+1}$ is *strict*, so that $p_i \neq p_{i+1}$. If there are arbitrarily long collections of such prime ideals, we say that R is *infinite-dimensional*.

In this problem, you may assume that for any commutative ring R, and any element $x \in R$ which is not a unit, there exists a maximal ideal of R containing x. (This is not obvious, and most proofs rely on the axiom of choice. If you're interested, look up "Zorn's Lemma.")

(a) Show that if R is a PID, then any non-zero prime ideal is a maximal ideal.

(b) Show that if R is a field, it has dimension zero. (If you have time, you should contemplate this fact in conjunction with the optional problem below which says maximal ideals are like points!)

(c) Show that if R is a PID and not a field, it has dimension one.

(d) Show that $\mathbb{Z}[x]$ is dimension two. (This requires a little bit of work.)

2. The Frobenius endomorphism

Let $\mathbf{k}$ be a field. Suppose there exists some positive integer n so that

$$n1 := 1 + \ldots + 1 = 0$$

in $\mathbf{k}$, where the summation has n terms. The smallest such n is a prime number. (If $n = ab$ with $a, b < n$, we'd have that $ab = 0$ in $\mathbf{k}$, while $a \neq 0$ and $b \neq 0$. This contradicts that $\mathbf{k}$ is a field, as fields have no zero divisors.) So we call the smallest such number p, and we say that $\mathbf{k}$ *has characteristic* p.

If there is no positive n for which $n1 = 0$ in $\mathbf{k}$, we say that $\mathbf{k}$ has characteristic 0.

Prove that if $\mathbf{k}$ is a field of characteristic $p \neq 0$, then the function

$$\varphi : \mathbf{k} \to \mathbf{k}, \qquad a \mapsto a^p = a \cdot \ldots \cdot a \ (p \text{ times })$$

is a ring homomorphism and an injection.

For future reference: The above φ is called the *Frobenius map* of the field $\mathbf{k}$.

3. An application of the Sylow theorems, Part I

Let p, q be prime numbers, and assume $q < p$. Let G be a group of order pq.

(a) Show that G has only one p-Sylow subgroup, and that it is normal. (Hint: If G acts on the set of p-Sylow subgroups by conjugation, and if you use the Sylow theorems...?)

(b) Assume that q does not divide $p-1$. Prove that G has only one q-Sylow subgroup.

(c) Assume that q does not divide $p-1$. Prove that G must be cyclic.

(d) Classify all groups of order 221.

4. An application of the Sylow theorems, Part II

You do not have to hand this problem in this week; it will be Problem 1 of the next (and last!) problem set.

Now suppose q divides $p-1$, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Let $\mathbb{A}$ be the set of all bijections $\mathbb{F}_p \to \mathbb{F}_p$ of the form $x \mapsto ax + b$, where $b \in \mathbb{F}_p$, and $a \in \mathbb{F}_p$ is an element such that $a^q = 1$. You don't need to verify it, but $\mathbb{A}$ is a group. Make sure you understand the composition law, though.

For this problem, you may assume that the group $(\mathbb{F}_p)^\times$ of units of $\mathbb{F}_p$ is cyclic. In fact, as we'll see, any finite field has a cyclic group of units.

(a) Show that $\mathbb{A}$ is a group of order pq.

(b) Show that $\mathbb{A}$ has trivial center.

(c) Show that a group of order pq, with q dividing $p-1$, is either cyclic or isomorphic to $\mathbb{A}$. (This requires some work!)

5. (Optional) Ideals are like subspaces

This problem explores a little bit of how rings connect with geometry. The take-away is that *ideals* are like *subspaces.*

Let $X \subset \mathbb{R}^n$ be a subset. For this problem, and for this problem only, we will say that a function $f : X \to \mathbb{R}$ is *continuous* if there exists a continuous function $\tilde{f} : \mathbb{R}^n \to \mathbb{R}$ extending f. (This only agrees with the usual definition of "continuous function on X" in special cases; but you can ignore that here.)

We let $C^0(X)$ denote the set of continuous functions $f : X \to \mathbb{R}$.

You should convince yourself that $C^0(X)$ is a commutative ring under the usual addition and multiplication of functions. The additive identity 0 is the function sending every $x \in X$ to $0 \in \mathbb{R}$, and the multiplicative identity 1 is the function sending every $x \in X$ to $1 \in \mathbb{R}$.

(a) Let $I \subset C^0(\mathbb{R}^n)$ be the subset of functions $\tilde{f}$ such that $\tilde{f}$ vanishes along X. Show that I is an ideal.

(b) Exhibit a ring isomorphism $C^0(\mathbb{R}^n)/I \cong C^0(X)$.

(c) Conclude that I is a prime ideal.

6. (Optional) Maximal ideals are like points

This problem also explores a little bit of how rings connect with geometry. The take-away is that *maximal ideals* are like *points.*

Let $X = S^1 \subset \mathbb{R}^2$ be the circle. Let R be the ring of continuous functions on X.

(a) For each $x \in X$, let $ev_x : R \to \mathbb{R}$ be the function sending $f \in R$ to $f(x) \in \mathbb{R}$. Show ev_x is a ring homomoprhism.

(b) For each $x \in X$, let $I_x \subset R$ be the set of continuous functions that vanish at x. Show that I_x is a maximal ideal.

(c) Exhibit an injection from the set X to the set of maximal ideals of R.

(d) Exhibit a bijection from the set X to the set of maximal ideals of R. You may need to look up something called Urysohn's Lemma.

7. (Optional) Think about maps $\mathbf{k}[x] \to R$ and repeat.

Let $\mathbf{k}$ be a field and R an integral domain. Fix a ring homomorphism $\mathbf{k} \to R$, and recall that this makes R a $\mathbf{k}$-vector space. Suppose $\dim_{\mathbf{k}} R$ is finite. Prove that R is a field.

8. (Optional) Fields of fractions

Let R be an integral domain. In this problem, you'll construct a "canonical" field that R includes into. (Someone in class asked if there was a way to "turn any ring into a field." This is pretty close to answering that question, and answers it exactly if the spirit is to create rings and fields that are related the way $\mathbb{Z}$ is related to $\mathbb{Q}$.)

(a) Consider the set $R \times (R \setminus \{0\})$ consisting of all pairs (a, b) such that $a, b \in R$ and $b \neq 0$. We declare a relation $(a, b) \sim (a', b')$ if and only if $ab' - a'b = 0$. Prove this is an equivalence relation.

Remark. It may help to visualize the equivalence class $[(a, b)]$ simply as a fraction $\frac{a}{b}$.

(b) Let $F = Frac(R)$ be the set of equivalence classes of the above relation. Show that the operations

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)], \qquad [(a, b)][(c, d)] := [(ac, bd)]$$

make F into a ring, where the additive identity is given by $[(0, b)]$ and the multiplicative identity is given by $[(1, 1)]$. Show also that F is a field.

(c) Show that the map $j : a \mapsto [(a, 1)]$ is a ring homomorphism from R to $Frac(R)$. Prove it is an injection.

(d) Show that the pair $(Frac(R), j)$ satisfies the following universal property: For any field F' and any ring homomorphism $j' : R \to F'$ that is an injection, there exists a unique homomorphism $g : Frac(R) \to F'$ such that

$$\begin{tikzcd}
R \arrow[r, "j'"] \arrow[d, "j"] & F' \\
Frac(R) \arrow[ur, dashed, "\exists ! g"'] &
\end{tikzcd}$$

commutes. (That is, $gj = j'$.)

Homework 12

Last one! Due Wednesday, November 29th, at 1:50 PM.

1. An application of the Sylow theorems, Part II

Let $q < p$ be primes. Last week, you showed that if q does not divide $p-1$, then any group of order pq is cyclic. In this problem, you'll finish the classification of groups of order pq by understanding the case that q does divide $p-1$.

So now suppose q divides $p-1$, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Let $\mathbb{A}$ be the set of all bijections $\mathbb{F}_p \to \mathbb{F}_p$ of the form $x \mapsto ax+b$, where $b \in \mathbb{F}_p$, and $a \in \mathbb{F}_p$ is an element such that $a^q = 1$. You don't need to verify it, but $\mathbb{A}$ is a group. Make sure you understand the composition law, though. (It's the composition of bijections.)

For this problem, you may assume that the group $(\mathbb{F}_p)^\times$ of units of $\mathbb{F}_p$ is cyclic. In fact, as we'll see, any finite field has a cyclic group of units.

(a) Show that $\mathbb{A}$ is a group of order pq.

(b) Show that $\mathbb{A}$ has trivial center.

(c) Show that a group of order pq, with q dividing $p-1$, is either cyclic or isomorphic to $\mathbb{A}$. (This requires some work!)

2. $F^\times$ is cyclic

(a) Let $\mathbf{k}$ be a field and let $f(x) \in \mathbf{k}[x]$ be a polynomial of degree d. Show that f has at most d roots in $\mathbf{k}$. (Hint: Each time there is a root a, you can factor $f(x)$ by the linear polynomial $(x-a)$.)

(b) Let F be a finite field of size q, and let $F^\times$ be the group of units of F. Show it has size $q-1$. (Note that q is not necessarily a prime; in general, you can see that if F is a field of characteristic p, it is a vector space over $\mathbb{F}_p$, so if q is finite, F is isomorphic to $(\mathbb{F}_p)^N$ as a group, for some N. So in general, $q = p^N$ for some N.)

(c) Using the classification of finitely generated abelian groups, consider the positive integers $s_1, \ldots, s_k$ for which

$$F^\times \cong C_{s_1} \times \ldots \times C_{s_k}$$

and where s_i divides s_{i+1}. Here, C_s is a cyclic group of order s—it is isomorphic to $\mathbb{Z}/s\mathbb{Z}$. Show that any element of C_{s_i} is a root of the polynomial $x^{s_i} - 1$.

(d) On the other hand, show that any element of $F^\times$ is a root to the polynomial $x^{q-1} - 1$.

(e) By counting possible roots, conclude that $k = 1$ and $s_1 = q-1$. Cnclude that $F^\times$ must be cyclic.

3. You're proving Jordan normal form

Let $\mathbf{k}$ be a field where every polynomial $f \in \mathbf{k}[x]$ admits at least one root. (Such a field $\mathbf{k}$ is called *algebraically closed.*) An example is $\mathbf{k} = \mathbb{C}$. There are others.

(a) Show that the only irreducible polynomials of $\mathbf{k}$ are linear. Using problems 1 and 2 of last homework, conclude that the only prime ideals of $\mathbf{k}[x]$ are of the form $(x-a)$ where $a \in \mathbf{k}$.

(b) Fix an integer $d \geq 1$ and consider the quotient *module* $V = \mathbf{k}[x]/(x-a)^d$. Show that this has the structure of a $\mathbf{k}$ vector space. Show that the collection

$$[1], [x-a], \ldots, [(x-a)^{d-1}]$$

is a basis for V (as a $\mathbf{k}$-vector space). In particular, you have shown that it is d-dimensional.

(c) Consider the $\mathbf{k}$-linear map which, for any $[g] \in V$, sends $[g]$ to $[xg] \in V$. Problems (d) and (e) have been combined. Show that in *the above basis, with orders swapped if necessary*, the map $[g] \mapsto [xg]$ can be written as a $d \times d$ matrix with a along the diagonal, 1's right above the diagonal, and 0's everywhere else.

4. Two equivalent formulations

Let R be a PID. Show that the following two logical statements are equivalent:

(a) For any finitely generated module M, there exists $k \geq 0$, $N \geq 0$, and ideals $(s_1), \ldots, (s_k) \in R$ such that

$$M \cong R^{\oplus N} \oplus (\oplus_{1 \leq i \leq k} R/(s_i))$$

and $(s_{i+1}) \subset (s_i)$ for $0 < i < k$. Moreover, the data of k, N, and the (s_i) are unique, in that $M \cong M'$ if and only if $N = N', k = k', (s_i) = (s_i')$.

(b) For any finitely generated module M, there exists $k \geq 0$, $N \geq 0$, prime ideals $p_1, \ldots, p_k$, and integers $a_1, \ldots, a_k \geq 1$ such that

$$M \cong R^{\oplus N} \oplus (\oplus_{1 \leq i \leq k} R/p_i^{a_i})$$

Moreover, the data of k, N, p_i and a_i are unique, in that $M \cong M'$ if and only if $N = N', k = k'$, and there exists some bijection $\sigma : \{i\} \cong \{i'\}$ so that $p_{\sigma i} = p_i', a_{\sigma i} = a_i'$.

Note that, given ideals I, J, the product ideal IJ is the ideal generated by all elements of the form xy for $x \in I, y \in J$. In particular, p^a is the ideal generated by elements of the form $x_1 \ldots x_a$ for $x_1, \ldots, x_a \in p$.

5. (Optional) Gaussian integers

You may want to compare to Problem 5 in Homework 9.

Let $\mathbb{Z}[i]$ be the set of all complex numbers $a + bi$ where a, b are integers. This set is called the *Gaussian integers*. Though you don't need to show it, this is a subring of $\mathbb{C}$.

(a) For any $z \in \mathbb{C}$, let $N(z) = |z|^2$. Show that $N(xy) = N(x)N(y)$ for any two $x, y \in \mathbb{C}$. Note that if $z \in \mathbb{Z}[i]$, then $N(z)$ is an integer.

(b) Find all units of $\mathbb{Z}[i]$.

(c) Recall that $x \in R$ is called prime if (x) is a prime ideal. Of the elements $2, 3, 5, 7, 11$ in $\mathbb{Z}[i]$, determine which are prime. (Numbers that used to be prime in $\mathbb{Z}$ need not be prime in $\mathbb{Z}[i]$!)

6. (Optional) Fermat's Little Theorem

Let F be a field of characteristic p, and consider the map $\varphi : F \to F$ given by $a \mapsto a^p$. You showed this was an injection, and a ring homomorphism, in Problem 2 of Homework 11. This φ is called the *Frobenius map.*

(a) Assume F is finite. Show that φ is a ring isomorphism from F to itself.

(b) Prove Fermat's Little Theorem: That for any element $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $a^p - a = 0$ in $\mathbb{F}_p$.

7. (Optional) Products of rings are like disjoint unions of spaces

(a) Given two sets X and Z, let $Fxn(X, Z)$ denote the set of functions form X to Z. Let X and Y be sets and $X \coprod Y$ their disjoint union. Exhibit a bijection

$$Fxn(X \times Y, Z) \cong Fxn(X, Z) \times Fxn(Y, Z).$$

That is, to give a function on $X \coprod Y$ is the same thing as giving a function on X, and on Y.

(b) Let R and S be rings. You don't need to prove it, but the direct product $R \times S$ is a ring with component-wise addition and multiplication:

$$(r, s) + (r', s') := (r + r', s + s'), \qquad (r, s)(r's') := (rr', ss')$$

Prove that if both R and S are not the zero ring, then $R \times S$ is never an integral domain (even if both R and S are).

(c) Let R be a commutative ring and let $Spec(R)$ denote the set of prime ideals of R. (Don't ask; for historical reasons, this set is called the *spectrum* of R.) Show that if S is another commutative ring,

$$Spec(R \times S) = Spec(R) \coprod Spec(S).$$

Math 122 Midterm One

Distributed Monday, Oct 2. Due Wed, Oct 11.

Problems 1-5 are worth 20 points each.

Optional problems are worth 10 points each.

Unfortunately, no collaborations. You can look at class videos and notes, but no online searches. You can ask CAs about concepts you've learned in class, but not about the specific contents of these problems.

1. A mystery

Let $\mathbb{Z}_{>0}$ be the set of all positive integers, and let F be the set of all functions $f : \mathbb{Z}_{>0} \to \mathbb{C}$ such that $f(1) \neq 0$. For every pair of elements $f, g \in F$, define $f \star g$ to be the function sending a positive integer n to the number

$$\sum_{(d_1,d_2)} f(d_1)g(d_2)$$

where the sum runs over all pairs of positive numbers (d_1, d_2) such that $d_1 d_2 = n$. Examples:

$$(f \star g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1).$$

$$(f \star g)(4) = f(1)g(4) + f(2)g(2) + f(4)g(1).$$

(a) Show that $\star$ is associative.

(b) Show that $f \star g = g \star f$.

(c) Show that $\star$ admits a unit—i.e., show there exists $e \in F$ so that $e \star f = f \star e = f$ for any f.

(d) Consider the function f which sends every n to the number $1 \in \mathbb{C}$. Determine whether f admits an inverse. That is, does there exist g such that $f \star g = g \star f = e$? If not, explain why not. If so, describe g.

(e) Is $(F, \star)$ a group?

2. Universal property of G/N_A

Fix a group G and fix a *subset* $A \subset G$. Let N_A be the intersection of all the normals subgroups of G containing A. As usual, we let $\pi : G \to G/N_A$ denote the quotient homomorphism.

For this problem, you may assume the universal property of quotient groups.

(a) Show that the group G/N_A (together with the map π) satisfies the following universal property: For any group L, and any group homomorphism $\phi : G \to L$ such that $\phi(a) = e_L$ for all $a \in A$, there exists a *unique* homomorphism $\psi : G/N_A \to L$ such that $\psi \circ \pi = \phi$.

(b) Assume there is some other group G', equipped with a group homomorphism $\pi' : G \to G'$ such that $A \subset \ker(\pi')$, satisfying the same universal property as above. (That is, for any $\phi : G \to L$ such that $A \subset \ker \phi$, there exists a unique $\psi' : G' \to L$ such that $\psi' \circ \pi' = \phi$.) Show that G' must be isomorphic to G/N_A.

3. This one's about clocks. (Really.)

(a) Let $\phi : G \to L$ be a surjective group homomorphism. Show that for every $l, l' \in L$, the pre-images $\phi^{-1}(l)$ and $\phi^{-1}(l')$ are in bijection. (Hint: If $\phi(g) = l$, how is the coset $g \ker \phi$ related to $\phi^{-1}(l)$? Then look back on your proof of Lagrange's Theorem.)

(b) Show that if A and B are abelian groups, and $\phi_1, \phi_2 : A \to B$ are group homomorphisms, then the map

$$\phi_1 + \phi_2 : A \to B \qquad (\phi_1 + \phi_2)(a) := \phi_1(a) + \phi_2(a)$$

is also a group homomorphism.

(c) Let $\mathbb{R}$ be the group of real numbers under addition. Let $2\pi\mathbb{Z} = \{0, \pm 2\pi, \pm 4\pi, \dots\} \subset \mathbb{R}$ be the subgroup of all real numbers that are integer multiples of the number 2π. Show that $\mathbb{R}/2\pi\mathbb{Z}$ is isomorphic to S^1.

For the next parts, make sure you're using previous parts of this problem.

Suppose it's currently 1:03. Let your clock run for twelve more hours, until it's 1:03 again.

(d) In that span of time, how many times does the minute hand of the clock aim at the exact same spot as the hour hand of the clock?

(e) Fix some angle $0 \leq \theta < 2\pi$. In the same span of time as above, how many times does the counterclockwise arc *from* the minute hand *to* the hour hand form an angle of exactly θ? (If θ happens to be exactly the angle formed at 1:03, only count *one* of the two instances of 1:03 occurring in the 12 hour period.)

4. Traces and group actions on $\{1, \ldots, n\}$

Fix a group G and a left action on the set $X = \{1, \ldots, n\}$. We suppose G is finite. For the sake of readability, if $i \in X$, we denote $g \cdot i \in X$ for the action of g on i. That is, using notation from class, $\mu(g, i) =: g \cdot i$.

For every $g \in G$, define an n-by-n matrix $\rho(g)$ as follows: the (i, j)th entry is 1 if and only if $g(j) = i$. Otherwise, the (i, j)th entry is 0. Equivalently, $\rho(g)$ is the matrix that takes the ith basis vector of $\mathbb{R}^n$ to the $(g \cdot i)$th basis vector of $\mathbb{R}^n$.

(a) Show that the assignment $g \mapsto \rho(g)$ is a group homomorphism from G to $GL_n(\mathbb{R})$.

Define the *trace* of a matrix to be the sum of its diagonal entries. We let $trace(A)$ denote the trace of A.

(b) Show that, for every $g \in G$, the quantity $trace(\rho(g))$ is the number of points of X fixed by g. (I.e., the number of those i such that $g \cdot i = i$.)

(c) Give an interpretation to the average

$$\frac{1}{|G|} \sum_{g \in G} trace(\rho(g)).$$

(It is equal to a meaningful quantity. It may be helpful to experiment when G is a subgroup of S_n generated by a single element; in that setting, you'll know what the group action looks like.) Prove that your interpretation is always correct!

5. Counting homomorphisms

In what follows, we let $\hom(G, H)$ denote the set of group homomorphisms from G to H.

(a) If G is finite, show that there is a unique group homomorphism from G to $\mathbb{Z}$.

(b) Suppose $G \cong H$. Exhibit a bijection between $Aut(G)$ and the set of group isomorphisms from G to H.

(c) Let m and n satisfy $gcd(m, n) = 1$. Show that there is a unique group homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$.

(d) For any three groups G, H_1, H_2, exhibit a bijection from $\hom(G, H_1 \times H_2)$ to the set $\hom(G, H_1) \times \hom(G, H_2)$.

(e) When G is *abelian*, exhibit a bijection from $\hom(H_1 \times H_2, G)$ to the set $\hom(H_1, G) \times \hom(H_2, G)$.

(f) Let $A(m)$ denote the number of group automorphisms of $\mathbb{Z}/m\mathbb{Z}$. Show that $A(mn) = A(m)A(n)$ if $gcd(m, n) = 1$. (Use parts (c)-(e).)

6. (Optional) More mattresses

Let R be a rectangular prism of length l, width w, and height h.

Recall from the first lectures that the symmetries of R, when $l \neq w$, $w \neq h$, and $l \neq h$, is called the *mattress group*. We call it M here.

It is a group of order 4, and you can verify that it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (For instance, see the solutions to an optional problem from weeks past.)

(a) Assume that $l = w$, but $h \neq w$. Show that the symmetries of such a mattress forms a group of order 8.

(b) Prove that this group is not isomorphic to Q_8.

(c) Assume that $l = w = h$, so your mattress is a cube. Show that the group of symmetries of this mattress has order 24.

(d) Write out the subgroup diagram for this group of order 24. Indicate which subgroups are normal.

7. (Optional) Hypermattresses

Let's define a *hypermattress* of dimension d to be the product of intervals $[-x_1, x_1] \times \ldots [-x_d, x_d] \subset \mathbb{R}^d$ where $x_i \neq x_j$ for $i \neq j$ and $x_i > 0$ for all i.

We let M_d, the hypermattress group of dimension d, be the group of rotational symmetries of a hypermattress of dimension d.

(a) Compute the order of M_d.

(b) Give a reasonable description of this group in terms of groups you've seen.

(c) Choose a partition of d:

$$d = n_1 + \ldots + n_k$$

where each $n_i \geq 1$. Assume that there are exactly k distinct positive numbers that appear in the list $(x_1, \ldots, x_d)$, where the ith distinct number appears n_i times. Compute the order of the group of rotational symmetries of the rectangular solid $[-x_1, x_1] \times \ldots \times [-x_d, x_d]$.

1. Coprime things

(a) Let G and H be finite groups, and assume $|G|$ and $|H|$ are coprime (i.e., their gcd is 1). Show that the trivial homomorphism is the only homomorphism from G to H.

(Hint: Lagrange's Theorem.)

Fix a homomorphism $\phi : G \to H$. By the first isomorphism theorem, $image(\phi) \cong G/\ker\phi$, so we have an equality of numbers $|image(\phi)| = |G|/|\ker\phi|$. This means $|image(\phi)|$ divides $|G|$. Since $image(\phi) \subset H$ is a subgroup of H, Lagrange's theorem says $|image(\phi)|$ also divides $|G|$. But the only positive integer dividing both is 1 since $|G|$ and $|H|$ are coprime. Since $image(\phi)$ consists of a single element, ϕ is the trivial homomorphism (sending all of G to $e_H \in H$).

(b) Let R and S be finite rings, and suppose that $|R|$ and $|S|$ are coprime. Further suppose that $|R|, |S| \geq 2$. Show there are no ring homomorphisms from R to S.

By above, the only group homomorphism from $(R, +)$ to $(S, +)$ is trivial. This means $1 \in R$ is sent to $0 \in S$—moreover, $0_S \neq 1_S$ since $|S| \geq 2$. Thus there is no function $\phi : R \to S$ which is simultaneously a group homomorphism and sends 1 to 1; this means there is no ring homomorphism from R to S.

2. Prime time

(a) Let $\phi : R \to S$ be a ring homomorphism, and $I \subset S$ an ideal. Show that the induced map

$$R/\phi^{-1}(I) \to S/I$$

is an injection. Here, $\phi^{-1}(I) \subset R$ is the pre-image of the ideal I. (This map is guaranteed to exist by the universal property of quotient rings.)

Let $\pi : S \to S/I$ be the quotient map and consider the composition $j : R \to S \to S/I$. The kernel of j is the set of all r which gets sent to $[0] \in S/I$—this is, by definition, the set of all r such that $\phi(r) = I$. In other words, $\ker(j) = \phi^{-1}(I)$. By the first isomorphism theorem, the induced function $R/\phi^{-1}(I) \to image(j)$ is an isomorphism, and in particular, an injection. Since $image(j) \subset S/I$, the function $R/\phi^{-1}I \to S/I$ is hence an injection.

(b) Suppose that $I \subset S$ is a prime ideal. Show that $\phi^{-1}(I)$ is a prime ideal.

If $I \subset S$ is prime, S/I has no zero divisors. Note that any subring of S/I must also have no zero divisors. Since $R/\phi^{-1}(I)$ is isomorphic to a subring of S/I by the first isomorphism theorem, it also has no zero divisors. Hence $\phi^{-1}(I)$ is a prime ideal of R.

3. Easy $p\mathbb{Z}$

Fix a prime number p.

(a) Let M be a module over $\mathbb{Z}/p\mathbb{Z}$. Show that any *subgroup* (not necessarily known to be a submodule) of M is automatically a submodule.

Let $N \subset M$ be a subgroup. It is closed under addition by definition. We must only show that for any $\underline{a} \in \mathbb{Z}/p\mathbb{Z}$ and any $x \in N$, the element $\underline{a}x$ is in N. By definition of module action, $\underline{1}x = x$, and $\underline{a}x = (\underline{1} + \ldots + \underline{1})x = x + \ldots + x$, where the summation happens a times. Since N is a subgroup, it is closed under addition, so $\underline{a}x = x + \ldots + x \in N$.

(b) Fix $n \geq 1$. Let

$$A = (\mathbb{Z}/p\mathbb{Z})^n = \mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}$$

be the direct product group. Show that any subgroup of A is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^m$ for some $0 \leq m \leq n$.

Since A is a finite set, it is finitely generated as a $\mathbb{Z}/p\mathbb{Z}$-module. By the above problem, any subgroup is also a $\mathbb{Z}/p\mathbb{Z}$ module, and finitely generated because a subset of a finite set is still finite. From class, we know any finitely generated $\mathbf{k}$-module admits a basis, hence is isomorphic to $\mathbf{k}^{\oplus m}$ for some finite m. Setting $\mathbf{k} = \mathbb{Z}/p\mathbb{Z}$, the result follows if we show $m \leq n$. This inequality holds because a subgroup must have fewer elements than A.

4. Take it to the max

(a) Let R be a commutative ring. Show that any maximal ideal of R is a prime ideal.

A field has no zero divisors: This is because if $ab = 0$ for $a, b \neq 0$, we have that $(a^{-1}a)b = 1b = b$ while $a^{-1}(ab) = a^{-1}0 = 0$, contradicting the assumption that $b \neq 0$. If R/I is a field, then, R/I is an integral domain. Hence I is prime.

(b) Exhibit a commutative ring R and a prime ideal $I \subset R$ which is not a maximal ideal.

Let $R = \mathbb{Z}$ and $I = (0)$. This is prime because R is an integral domain ($xy = 0$ implies either x or y is 0) and (0) is not maximal because $\mathbb{Z}/(0) \cong \mathbb{Z}$ is not a field.

5. True or False?

You must give a justification for your answers.
(a) The ideal generated by x is a maximal ideal in $\mathbb{Z}[x]$.

False. Two solutions: The quotient $\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}$, which is not a field. (To see the isomorphism, apply the first isomorphism theorem to the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}, x \mapsto 0$.) Second solution: The ideal $(2, x)$ contains 2 but not 1, so is bigger than (x) but is proper; so (x) is not maximal.

(b) The ideal generated by x is a maximal ideal in $\mathbb{R}[x]$.

True. The ring homomorphism $\mathbb{R}[x] \to \mathbb{R}$ given by sending $x \mapsto 0$ has kernel (x), and by the first isomorphism theorem, $\mathbb{R}[x]/(x)$ is a field.

(c) For any commutative ring R and any $n \times n$ matrix A with entries in R, A satisfies its characteristic polynomial.

True. This is the Cayley-Hamilton Theorem.

(d) There exists an element of order 6 in $GL_2(\mathbb{Z})$.

True. Here, you just had to exhibit an example, but an example is very hard to come by. The trick is to find an element of order 3 (that's the hard part), and an element of order 2—then you can *hope* that their product must have order 6 by usual group theory. If the two elements commute with each other, then you *know* that the product has order 6 by usual group theory.
To think of an element of order 3, you either have to be lucky, or very clever—for instance, by Cayley-Hamilton, you need to think of a polynomial that divides $x^3 - 1$. Since 1 is a root, you can divide $x^3 - 1$ by $(x - 1)$ to arrive at $f = x^2 + x + 1$. This means you seek matrices with trace -1 and determinant 1. An example of such a thing is $A = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$. It's invertible because 1 is a unit in $\mathbb{Z}$.
An element of order 2 is easy to come by; for instance, the matrix $-I$ with -1 along the diagonal and 0s elsewhere. Moreover, because the matrix $-I$ is diagonal, it commutes with all other matrices! So we conclude that $-A$ is an element of order 6.

6. (Optional) Counting is hard.

Let p be a prime number. Let V be a vector space over $\mathbb{Z}/p\mathbb{Z}$ of dimension k.

For each $0 \leq d \leq k$, compute the number of subspaces $W \subset V$ of dimension d.

This is a fun one. First, instead of computing the number of subspaces, let's compute the number of collections of d ordered linearly independent elements. This is, using the same reasoning from your homework,

$$A = (p^k - 1)(p^k - p)\dots(p^k - p^{d-1}).$$

Now, the group $GL_d(\mathbb{Z}/p\mathbb{Z})$ acts on this collection—two linearly independent collections U and V define the same subspace if and only if there is a linear transformation sending U to V; there are $B = |GL_d(\mathbb{Z}/p\mathbb{Z})|$ many such transformations. So we arrive at the number A/B. Writing it out, we have

$$A/B = \frac{(p^k - 1)(p^k - p)\dots(p^k - p^{d-1})}{(p^{d-1} - 1)\dots(p^{d-1} - p^{d-2})}.$$

7. (Optional) $\mathbb{F}_9$

(a) Show that x^2+1 generates a maximal ideal in $\mathbb{Z}/3\mathbb{Z}[x]$.

Let $f = x^2+1$. Fix any g which is not in the ideal (f) generated by f. We want to show that any ideal I for which $g \in I, (f) \subset I$ must be all of the ring. Writing $g = fh + r$, r must be a polynomial of degree < 2, and $r \in I$. Now there are two cases to check. Case One: If r is degree 0, r must be a non-zero element of $\mathbb{Z}/3\mathbb{Z}$ (else $g \in (f)$), hence $1 \in I$, meaning I is the whole ring. Case Two: If r is degree 1, we now write $f = qr + p$. Note that a linear polynomial r cannot divide f because f has no roots in $\mathbb{Z}/3\mathbb{Z}$ as one can check. Hence p must be a non-zero constant, and $p = f - qr \in I$, so this means I is the whole ring.

(b) Exhibit a field with 9 elements.

Since $f = x^2+1$ generates a maximal ideal, consider $\mathbb{Z}/3\mathbb{Z}[x]/(f)$. This is a field. Moreover, as with homework, it's a vector space over $\mathbb{Z}/3\mathbb{Z}$ with basis $[1], [x]$. A two-dimensional vector space over $\mathbb{Z}/3\mathbb{Z}$ has 9 elements.

8. (Optional) Double trouble.

Let G be a group such that every element has order 2. Show that G must be abelian.

If every element has order 2, every element is its own inverse. Hence

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

where the middle equality uses a general fact about inverses in groups.

9. (Optional) This seems important...

Let $R = \mathbb{C}[x, y]$ be the polynomial ring in two variables, and let $f = y - g(x)$ where $g(x)$ is some polynomial in x. Exhibit a ring isomorphism between

$$R/(f)$$

and the ring

$$\mathbb{C}[x].$$

Consider the ring homomorphism $\phi : R \to \mathbb{C}[x]$ given by

$$\sum a_{ij} x^i y^j \mapsto \sum a_{ij} x^i (g(x))^j.$$

It is certainly a surjection; any element of the target is hit by a polynomial with no y term. The kernel obviously contains f, so contains (f) because kernels are ideals.

Consider also the homomorphism $\psi : \mathbb{C}[x] \to R/(f)$ given by sending

$$\sum b_i x^i \mapsto [\sum b_i x^i].$$

We see that $\phi \circ \psi = \mathrm{id}_{\mathbb{C}[x]}$, which shows ϕ is also an injection. We conclude ϕ is an isomorphism.

10. (Optional) WER

What musical meme has been appearing throughout our classes?

If you don't know the answer, I'm not giving it away here.

Write your name here:

Math 122 Final

Logistics. This exam will be scored out of 200 points. You will note that the total amount of points to be earned in the non-optional problems is 240, so you have wiggle room to not fully complete the non-optional problems.

This exam is structured as two dinners—a ring dinner and a group dinner (lol)—where the desserts of both are optional problems. Most dessert problems are more difficult than the usual dinner problems, though there are some sweets thrown in.

As usual, I recommend you start early. This exam is due Thursday, December 14, at 11:59 PM (i.e., right before the midnight between Thursday and Friday). This exam cannot be finished in one night, and I recommend that you manage your 16 days with this exam wisely.

As with the second midterm, if the average is lower than expected, I will add a lump sum to every score to achieve at least a C+ average. If the average is higher than expected, the scores will remain as-is.

Resources. You may only use course notes and videos and past homeworks. *You are allowed to collaborate* on the entirety of this exam, but as usual, the act of writing up the solutions must be done completely on your own.

Ring Dinner

1. Pre-dinner hors d'oeuvre: Show me you can do it (20 points)

For the following classifications, write out the groups in the two forms we've studied:

$$\bigoplus_i \mathbb{Z}/p_i^{a_i}\mathbb{Z}, \qquad p_i \text{ prime} \qquad\text{and}\qquad \bigoplus_j \mathbb{Z}/s_j\mathbb{Z}, \qquad s_j|s_{j+1}.$$

(a) (10 points.) Classify all abelian groups of order 81.

(b) (10 points.) Classify all abelian groups of order 360.

2. Appetizer: Some easy finite fields (40 points)

Let p be a prime number and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(a) (10 points.) Show that if F is another field with exactly p elements, it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (as a ring). This shows that any two fields with exactly p elements are isomorphic.

(b) (10 points.) Show that there exists at least one irreducible polynomial of degree 2 in $\mathbb{F}_p[x]$.

(c) (10 points.) For every prime p, prove that there exists a field with exactly p^2 elements.

(d) (10 points.) Show that any two fields with exactly p^2 elements are isomorphic.

3. Main course: Ring, ring! (60 points)

(a) (20 points.) Let R be a commutative ring and m_1, m_2 two distinct maximal ideals. Let $I = m_1 \cap m_2$. Show that R/I is the direct product of two fields.

(b) (20 points.) Find all values of $a, b \in \mathbb{Z}/3\mathbb{Z}$ so that the quotient ring

$$\mathbb{Z}/3\mathbb{Z}[x]/(x^3 + x^2 + ax + b)$$

is a field. Justify your answer.

(c) (20 points.) Let R be an integral domain. Show that $R[x]$ is a principal ideal domain if and only if R is a field.

4. Dessert: Nilpotence (10 points)

Let R be a commutative ring, with $0 \neq 1$. You will likely invoke Zorn's Lemma in this problem.

(a) (5 points.) An element $x \in R$ is called *nilpotent* if $x^n = 0$ for some $n \geq 1$. Show that x is nilpotent if and only if it is contained in every prime ideal of R.

(b) (5 points.) Show that the set of all nilpotent elements is an ideal of R.

5. Dessert: Matrices and their ideals (10 points)

Let R be a commutative ring and fix an integer $n \geq 1$. We let $M(R) = M_{n\times n}(R)$ be the (non-commutative) ring of n-by-n matrices with entries in R. If $I \subset R$ is an ideal of R, we let $M(I)$ denote the set of matrices with entries in I.

(a) (5 points.) Show that for any ideal I, $M(I)$ is a two-sided ideal of $M(R)$. Conversely, prove that any two-sided ideal of $M(R)$ is of the form$M(I)$.

(b) (5 points.) Fix an ideal $I \subset R$. Can you find a relationship between the quotient ring $M(R)/M(I)$ and the matrix ring $M(R/I)$?

6. Dessert: Units of $\mathbb{F}_{16}$ (20 points)

(a) (5 points.) By finding an irreducible polynomial of degree 4 over $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, exhibit a field $\mathbb{F}_{16}$ with 16 elements.

(b) (5 points.) By homework, you know that $\mathbb{F}_{16}^\times$ is cyclic. Find all elements which generate this cyclic group.

(c) (10 points.) Compute the number of ring automorphisms of $\mathbb{F}_{16}$. (The previous part may only help for guidance; this is not very easy with our present knowledge in this class.)

7. Dessert: Homework 12, Problem 4 (20 points)

Do Homework 12, Problem 4, for an arbitrary PID R. This is not easy, and you will most likely need to prove the following two statements:

(a) If $gcd(a, b)$ is a unit, then $R/(a) \oplus R/(b) \cong R/(ab)$, and

(b) For any $s \in R$, there exists a *unique* collection of distinct prime ideals $(p_1), \dots, (p_k)$ and a unique collection of integers $a_i \geq 1$ such that

$$(s) = (p_1)^{a_1} \dots (p_k)^{a_k}.$$

(A stronger statement, that unique prime factorization holds at the level of elements, not the level of ideals, is indeed true.) (b) will in turn rely on the following, which you also will need to prove:

(c) Any increasing sequence of ideals $I_1 \subset I_2 \subset \dots$ in a PID eventually stops—that is, there exists some N for which $I_N = I_{N+1} = \dots$.

We say that a ring satisfying (c) is a *Noetherian ring*, and you are proving that any PID is a Noetherian ring. This is named after Emmy Noether.

Group Dinner

1. Pre-dinner hors d'oeuvre: Show me you can do it (20 points)

For every prime p, find all p-Sylow subgroups of S_5. (For full credit: For each p-Sylow subgroup, write out the elements of each subgroup in a reasonable way and indicate how many p-Sylow subgroups there are for each p.)

2. Appetizer: More Sylow stuff (40 points)

(a) (20 points.) Let $|G| = p^n a$ where p does not divide a. By studying the proof of the Sylow theorems from class, show that the number of p-Sylow subgroups of G divides a. (This is another powerful fact, often stated as part of the Sylow theorems.)

(b) (10 points.) Prove that there is *no* non-abelian simple group of order 54.

(c) (10 points.) Show that any group of order 12 has at least one normal Sylow subgroup.

3. Main course: Groups acting on their cosets (60 points)

Let $H \subset G$ be a subgroup and assume that (even if G and H are not finite) the set G/H is finite. We call its size N. Recall from class that this N is called the *index* of H in G, and is sometimes written

$$[G : H].$$

(a) (10 points.) Show that left multiplication $G \times G/H \to G/H$ defined by

$$(g, g'H) \mapsto (gg')H$$

is a group action of G on G/H. By choosing an ordering of the elements of G/H, exhibit a group homomorphism $\phi : G \to S_N$.

(b) (10 points.) Show that the kernel of ϕ is contained in H.

(c) (20 points.) Show that $[G : H][H : kernel(\phi)] = [G : kernel(\phi)]$. (This is true for any sequence of subgroups $K \subset H \subset G$, each of finite index.)

(d) (20 points.) Assume that $[G : H]$ is a prime number p, and that p is the smallest prime number dividing $|G|$. Prove that H is a normal subgroup of G.

4. Dessert: Dihedral groups (10 points)

You classified all groups of order pq in homework. In particular, for dihedral groups of order D_{2p} where p is an odd prime, you know D_{2p} is isomorphic to a group which we'll denote as $\mathbb{A}_p$. (It is the group of bijections from $\mathbb{F}_p$ to itself of the form $x \mapsto ax + b$ where a is a square root of 1 in $\mathbb{F}_p$.)

(a) (5 points.) Write an explicit isomorphism from D_{2p} to the group $\mathbb{A}_p$.

(b) (5 points.) Find the number of such isomorphisms.

5. Dessert: Innies and Outies (10 points)

Recall that for any group G, conjugation defines a homomorphism $G \to Aut(G)$. This sends an element g to the automorphism $x \mapsto gxg^{-1}$.

Let $Inn(G) \subset Aut(G)$ denote the image of this homomorphism. An element of $Inn(G)$ is called an *inner automorphism* of G.

(a) (5 points) Show that $Inn(G)$ is a normal subgroup of $Aut(G)$.

(b) (5 points) Let $Out(G) := Aut(G)/Inn(G)$ be the quotient group. Show that if $G = S_n$ and $n \neq 2, 6$, the group $Out(G)$ is trivial.

An element of $Aut(G)$ which is not contained in $Inn(G)$ is called an *outer automorphism* of G.

6. Dessert: Why is 6 so special? (20 points)

(a) (5 points) Show that S_5 has six 5-Sylow subgroups.

(b) (5 points) Since any group acts on the set of its p-Sylow subgroups by conjugation, the conjugation action of S_5 on its 5-Sylow subgroups gives a homomorphism $S_5 \to S_6$. We'll call its image H. Show that S_6 has six subgroups that are conjugate to H (including H itself).

(c) (10 points) Thus S_6, acting by conjugation on the six conjugate subgroups of H, has a map $S_6 \to S_6$. Show that this is an *outer* automorphism from S_6 to itself.