Practice problems for Midterm 1

The midterm will take place Wednesday, October 15th, right after Columbus Day weekend.

1. Definitions

Know the definitions of the following. [2]

(a) Group
(b) Subgroup
(c) Order of an element
(d) Order of a group
(e) Group homomorphism
(f) Group isomorphism
(g) Kernel
(h) Image
(i) Normal subgroup
(j) Conjugation by h
(k) Conjugacy class of an element of a group
(l) $\mathrm{Aut}_{\mathcal{S}et}(X)$
(m) Group action on a set X.
(n) Orbit
(o) Orbit space
(p) Index of a subgroup (be precise!)
(q) Stabilizer
(r) Center of a group
(s) Abelian group
(t) When H is normal, the group operation on G/H.

[2] If you are like me, you may also despise the memorization aspect of math. I've always disliked how tests force you to memorize. But we need a common and efficient language to speak of complex ideas, and this section is meant to make sure that you can communicate using the language on which English-speaking mathematicians have come to agree. Moreover, I hope that some of these ideas become intuitive enough that you will even be able to *guess* the correct definition, based on how we have come to know these words.

(u) $\mathbb{Z}/n\mathbb{Z}$
(v) S_n
(w) A_n
(x) Simple group

2

(a) Prove that the kernel of any group homomorphism is a normal subgroup.

3

(a) Show that if two cyclic groups have the same order (finite or not), they must be isomorphic.

4

(a) Exhibit an explicit element τ showing that $(123)(45)$ and $(253)(16)$ are conjugate in S_6.
(b) Show that S_n has at least n distinct subgroups of order $(n-1)!$.
(c) Write down every subgroup of S_3 explicitly. That is, what are the subsets of S_3 that are subgroups? When you write elements of S_3, use cycle notation.

5

(a) If S is a finite set, show that the free group on S is finitely generated.
(b) Prove that any finite group is finitely generated.

6

(a) Show that $\mathbb{Z}$ is not simple.
(b) Show that S_3 is not simple.
(c) Show that $\mathbb{Z}/12\mathbb{Z}$ is not simple.
(d) Show that A_4 is not simple.

7

(a) Let H be the subgroup of S_5 generated by $(13)(245)$. Write down every element of H.
(b) Compute the index of H inside S_5.

8

(a) State the first isomorphism theorem.
(b) State Lagrange's theorem.

9

Show by example that a subgroup of a simple group need not be simple. (You may assume that A_5 is simple.)

10

Recall that the Hamiltonians, or the quaternions, is the name for $\mathbb{R}^4$ equipped with the following operation: If $(s, \vec{u})$ and $(t, \vec{v}) \in \mathbb{R} \times \mathbb{R}^3 \cong \mathbb{R}^4$ are elements, we define

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

Here, $\vec{u} \cdot \vec{v}$ indicates the dot product of $\vec{u}$ with $\vec{v}$. In the last coordinate, $\vec{u} \times \vec{v}$ is the cross product in $\mathbb{R}^3$.

Let S^3 denote those elements $(s, \vec{u}) \in \mathbb{R}^4$ for which $s^2 + |\vec{u}|^2 = 1$. Show that S^3 is a group under the above multiplication. Show that S^3 is not an abelian group.

11. Short exact sequences

Show that following sequences do not split:

(a) $\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for $n \neq 0, \pm 1$.

(b) $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ where $\phi([0]) = [0]$ and $\phi([1]) = [2]$.

12

If n and m are relatively prime (meaning they share no common divisors aside from 1) show that $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(nm)\mathbb{Z}$.

1. Some things you've (maybe) done before. 5 points each.

(a) If g and h are elements of a group G, show that $(gh)^{-1} = h^{-1}g^{-1}$.

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1}\\ &= g1g^{-1}\\ &= gg^{-1}\\ &= 1.\end{aligned}$$

Likewise,

$$\begin{aligned}(h^{-1}g^{-1})(gh) &= h^{-1}(g^{-1}g)h\\ &= h^{-1}1h\\ &= h^{-1}h\\ &= 1.\end{aligned}$$

(b) Show that the identity element of a group is unique.

If both 1 and 1' satisfy the property of being an identity, we know $1g = g$ for all g and $h1' = h$ for all h. Taking $g = 1'$ and $h = 1$, by transitivity of equality we have that $1 = 1'$.

2. You are now a Level Two Group Theorist. 5 points each.

(a) Consider the element $\sigma = (13467)$ inside S_9. What is the order of σ? (Give some reasoning.)

By *definition*, recall that a cycle is represented by the notation

$$(i\,\sigma(i)\sigma^2(i)\ldots\sigma^{|\sigma|-1}(i))$$

for some $i \in \underline{n}$ in the non-trivial orbit of σ. Hence the number of terms in the cycle notation is equivalent to the order of σ. In this case, there are five terms inside the parentheses. So the order is five.

(b) Using Lagrange's Theorem, show that any finite group with prime order $p \geq 2$ must be cyclic.

Let $g \in G$ be any element that is not the identity. The subgroup $\langle g \rangle$ must have order dividing $p = |G|$ by Lagrange's Theorem, but the only numbers dividing a prime number are 1 and p itself. On the other hand, we know that $|\langle g \rangle| \geq 2$ since this subgroup contains at least two distinct elements: 1_G and g itself. Hence $|\langle g \rangle| = p$, meaning $\langle g \rangle = G$.

3. Some (not) normal subgroups. 10 points each.

(a) Show that the subgroup generated by (123) in S_3 is normal.

This element has order 3, being a cycle of length 3. Hence it is a subgroup of index 2. (This follows from the proof of Lagrange's Theorem: $|S_3|/|\langle(123)\rangle| = 6/3 = 2$.) By homework, any subgroup of index 2 is normal. Alternatively, the group generated by (123) is A_3, so it's the kernel of a group homomorphism.

(b) Show that the subgroup generated by (123) in S_4 is *not* normal.

We know that two elements of S_n are conjugate if and only if they have the same cycle shape. Well, the cycle (124) (for instance) has the same cycle shape as (123). However,

$$\langle(123)\rangle = \{1, (123), (132)\}.$$

So (124), a conjugate of (123), is not inside $\langle(123)\rangle$. We are finished. If you want to show that (123) is a conjugate of (124) explicitly, one can compute that

$$\tau(123)\tau^{-1} = (124)$$

where $\tau = (34)$:

$$\begin{aligned}(34) \circ (123) \circ (34) &= (34) \circ (3412) \\ &= (412) \\ &= (124).\end{aligned}$$

4. Simple is simple. 10 points.

Let G be a simple group. Show that any group homomorphism from G to another group H must either be an injection, or trivial. (Trivial here means that all of G is sent to a single element of H.)

Since G is simple, its only normal subgroups are $\{1\}$ and G itself. But a kernel of a homomorphism $\phi : G \to H$ is always a normal subgroup, so any homomorphism ϕ must have kernel equal to $\{1\}$ (in which case ϕ is injective) or equal to G (in which case all of G is sent to the identity of H).

5. Some group diversity. 10 points.

For any $n \geq 3$, exhibit two groups G_n and H_n of order $n!$ which are not isomorphic. (You must explain why they are not isomorphic.)

Let $G_n = \mathbb{Z}/n!\mathbb{Z}$, and let $H = S_n$. The former is abelian, while the latter is not for $n \geq 3$, so these two groups cannot be isomorphic.

6. Extra Credit. Normal subgroups of quotients, I. 5 pts each.

Let $\phi : G \to H$ be a surjective group homomorphism.

(a) Show that if $K \subset G$ is normal, then $\phi(K) \subset H$ is normal.

We need to show that $h\phi(K)h^{-1} \subset \phi(K)$ for all $h \in H$. (We showed in class that this implies $h\phi(K)h^{-1} = \phi(K)$ for all h.)

Well, since ϕ is a surjection, there exists an element $g \in G$ for which $\phi(g) = h$. So for any $k \in K$, we have that

$$h\phi(k)h^{-1} = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\phi(k)\phi(g^{-1}) = \phi(gkg^{-1}).$$

Since $K \subset G$ is normal, we know that $gkg^{-1} = k'$ for some $k' \in K$. Hence $\phi(gkg^{-1}) = \phi(k') \in \phi(K)$.

We've show that for every element $\phi(k) \in \phi(K)$, and for every $h \in H$, $h\phi(k)h^{-1} \in \phi(K)$. This completes the proof.

(b) Show that any normal subgroup $L \subset H$ equals $\phi(K)$ for some normal subgroup $K \subset G$.

Let

$$K = \{k \in G \text{ such that } \phi(k) \in L\}.$$

We must show that K is normal. So for any $g \in G$ and $K \in K$, we must show that $gkg^{-1} \in K$. Well,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} \in L$$

since L is normal in H. Hence $gkg^{-1} \in K$. This completes the proof.

7. Extra Credit. Normal subgroups of quotients, II. 10 pts.

Let $\phi : G \to H$ be a surjective group homomorphism as before. Show that there is a bijection between the set

$$\{K \subset G \text{ such that } K \text{ is a normal subgroup containing } \ker \phi\}$$

and the set

$$\{L \subset H \text{ such that } L \text{ is a normal subgroup of } H.\}.$$

For sanity, let us call the first set $\mathcal{K}$, and the second set $\mathcal{L}$. In (b) of the last problem we exhibited a function

$$j : \mathcal{L} \to \mathcal{K}$$

by sending

$$L \mapsto j(L) = \{k \in G \text{ s.t. } \phi(k) \in L\}.$$

(In the previous problem, $j(L)$ was called K.) Note that $j(L)$ contains the kernel of ϕ, since it in particular contains all k that map to $1 \in L$. We must show that j is a bijection.

On the other hand, by (a) of the last problem, we have a function

$$h : \mathcal{K} \to \mathcal{L}$$

sending $K \mapsto \phi(K)$. Let us show that j and h are inverse to each other. That $h \circ j = \mathrm{id}_{\mathcal{L}}$ is obvious—for $h(j(L))$ is the image of all elements that map to L, i.e., L. Now we must prove that $j(h(K)) = K$.

For simplicity of notation, let $h(K) = L$. If $g \in j(L)$, $\phi(g) \in L$ by definition of $j(L)$. On the other hand, $\phi(K) = L$, so there is some $k \in K$ such that $\phi(g) = \phi(k)$. This means that $\phi(gk^{-1}) = 1_L$, so $gk^{-1} = x$ is in the kernel of ϕ. But both K and $j(L)$ contain the kernel of ϕ, so by closure of subgroups, we must have that $g = xk \in K$, and $k = gx^{-1} \in j(L)$. This shows $j(h(K)) \subset K$ and $K \subset j(h(K))$. We are finished.

8. Extra Credit. 5 points each.

(a) State Mordell's Theorem. (You may use the word "nice" without defining it. You do not need to prove anything.)

Let $f(x)$ be a nice cubic polynomial with rational coefficients. Then $\mathbb{E}(\mathbb{Q})$ is finitely generated.

(b) What is the fundamental group of $\mathbb{R}^3$ with two disjoint lines removed? (You do not need to prove it; you may just state the answer.)

The free group on two generators.

Math 122 Midterm 2 Fall 2014

Instructions

- Due: Wednesday, Dec 3, by noon (class time).
- You may use your class notes, my class notes, your past homework, homework solutions, and midterm solutions. But do not ask for help (or look for answers) on stack exchange, on math overflow, or on any other online source.
- All collaboration and writing policies in the syllabus apply.
- You may collaborate on Problems 1 - 6. You may not collaborate on the rest: Problems 7 - 12. The seemingly difficult problems are loads of fun to solve, so I encourage you to persist.
- Start early. Think deeply. Have fun.

1. Irreducibility

Let F be a field. For any $x \in F$, note that there is a function

$$F[t] \to F,$$

called *evaluation at* x. Explicitly, if $f = a_d t^d + \dots a_1 t + a_0$ is a polynomial, we send f to

$$f(x) = a_d x^d + \dots a_1 x + a_0 \in F.$$

Here, by x^d, we mean of course the element of F obtained by multiplying x with itself d times.

(a) Show that for any $x \in F$, evaluation at x is a ring homomorphism.

(b) Show that f can be factored by a linear polynomial if and only if there is some $x \in F$ for which $f(x) = 0$. (Hint: Use the division algorithm and induct on degree.)

Recall that a polynomial $f(t) \in F[t]$ is *irreducible* if the only polynomials dividing $f(t)$ are degree 0 (i.e., are constants) or have degree equal to f.

(c) If $F = \mathbb{C}$, show that $f(t) = t^2 + 1$ is not irreducible.

(d) If $F = \mathbb{R}$, show that $f(t) = t^2 + 1$ *is* irreducible. (Hint: If $f(t) = g(t)h(t)$, what can you say about the degrees of g and h? And what does that say about solutions to $f(t)$?)

(e) For each of the primes $p = 2, 3, 5, 7$, indicate which of the following polynomials has a solution in $\mathbb{Z}/p\mathbb{Z}$. (You'll need to just compute.)
   (a) $t^2 + \overline{1}$ (i.e., which of these finite fields has a square root to -1?)
   (b) $t^3 - \overline{2}$ (i.e., which of these fields has a cube root to 2?)
   (c) $t^2 + t + 1$ (i.e., for which of these fields does this polynomial factor?)

2. Principal ideal domains

Let R be an integral domain. We call R a *principal ideal domain* if every ideal $I \subset R$ is equal to (x) for some $x \in R$. That is, every ideal is generated by a single element.

(a) Show that $\mathbb{Z}$ is a principal ideal domain. (We've done this in class, so you can do it, too!)
(b) Let F be a field. Show that $F[t]$ is a principal ideal domain. (Hint: If $I \neq (0)$, let n be the least degree for which a degree n polynomial is in I. If $p(t)$ and $q(t)$ are both degree n polynomials, how are they related? Finally, given any $f(t) \in I$, what happens when you divide $f(t)$ by $p(t)$ and look at the remainder?)

3. The second isomorphism theorem

Fix a group G. Let $S \subset G$ be a subgroup, and $N \triangleleft G$ be a normal subgroup.

(a) Let SN be the set of all elements in G of the form sx where $s \in S$ and $x \in N$. Show this is a subgroup of G.
(b) Show that N is a normal subgroup of SN.
(c) Show that $S \cap N$ is a normal subgroup of S.
(d) Exhibit an isomorphism between $S/(S \cap N)$ and SN/N. (Hint: Does the equivalence class $[s]$ in the former group define an equivalence class $[sn]$ in the latter group? Does the n in $[sn]$ matter?)

4. Subgroups descend to quotient groups

Let G be an arbitrary group, and $H \triangleleft G$.

(a) Show that there is a bijection between the set of subgroups in G containing H, and the set of subgroups in G/H.
(b) Show that there is a bijection between the set of *normal* subgroups in G containing H, and the set of normal subgroups in G/H. (This time, this isn't extra credit.)

5. Solvable groups

A group G is called *solvable* if there exists a finite sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian.

(a) Show that any abelian group is solvable. (If this seems trivial, it's because it is.)
(b) Show any group of order pq, where p and q are distinct primes, is solvable.

(c) Show that if G is simple and non-abelian, G cannot be solvable.

The following is a great application of the isomorphism theorems, and of the previous problem.

(d) Show that if G is solvable, so is any subgroup of G.

(e) Show that if G is solvable, and $K \subset G$ is normal, then G/K is solvable.

6. $GL_n(\mathbb{F}_q)$

Let $\mathbb{F}_q$ be a finite field with q elements.

(a) Let $V = \mathbb{F}_q^n = \mathbb{F}_q^{\oplus n}$ be an n-dimensional vector space over $\mathbb{F}_q$. Show that $G = GL_n(\mathbb{F}_q)$ acts *transitively* on $V - \{0\}$. (That is, show that for any pair $x, y \in V$, there is some group element g so that $gx = y$.)

(b) Prove that $G = GL_n(\mathbb{F}_q)$ has

$$\left(\prod_{k=1}^{n}(q^k - 1)\right)\left(\prod_{k=1}^{n-1} q^k\right)$$

elements in it. (You can either count intelligently, or apply the orbit-stabilizer theorem inductively. Either way, use matrices.)

(c) Show that $GL_n(\mathbb{F}_q)$ has a normal subgroup of index $q - 1$. (Hint: The determinant is still a group homomorphism.)

(d) Consider $G = GL_2(\mathbb{F}_q)$. Assume p is the unique prime number dividing q. [1] Show that $|\operatorname{Syl}_p(G)|$ cannot equal 1. (Try thinking about upper-triangular and lower-triangular matrices, then think about special cases of them.)

(e) How many elements of order 3 are in $GL_2(\mathbb{F}_3)$? (You may want to start by determining the number of Sylow 3-subgroups. Either way, dig in.)

No more collaboration

7. Ring homomorphisms

(a) Show that a composition of two ring homomorphisms is a ring homomorphism.

(b) For a ring R, let $M_{k\times k}(R)$ denote the ring of $k \times k$ matrices with entries in R. Specifically, if (a_{ij}) is a matrix whose i, jth entry is a_{ij}, we define

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \qquad (a_{ij})(b_{ij}) = (\sum_{l=l}^{k} a_{il}b_{lj}).$$

[1] One can prove that any finite field has size p^k for some prime p. As pointed out to me by Kevin, it's not hard—a finite field of characteristic p is a module over $\mathbb{Z}/p\mathbb{Z}$, so is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. But how many elements must such a set have?

Show that if $f : R \to S$ is a ring homomorphism, then the function

$$F : M_{k\times k}(R) \to M_{k\times k}(S), \qquad (a_{ij}) \mapsto (f(a_{ij}))$$

is a ring homomorphism.

(c) Prove that

$$f(\det A) = \det(F(A)).$$

You may want to start by proving it for $k = 1$, then perform induction using the cofactor definition of determinants.

8. Invertible matrices

Let S be a ring. We say $x \in S$ is a *unit* if there is a multiplicative inverse to x—i.e., an element $y \in S$ so that $xy = yx = 1_S$. As an example, if S is the ring of $k \times k$ matrices in some ring R, then a matrix is invertible if and only if it is a unit.

(a) Determine which of the following matrices is a unit in $M_{k\times k}(\mathbb{Z})$:

$$\begin{pmatrix} 2 & 5 \\ 4 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix}$$

(b) For the primes $p = 2, 3, 5$, consider the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ sending $a \mapsto \overline{a}$. This induces a ring homomorphism $M_{k\times k}(\mathbb{Z}) \to M_{k\times k}(\mathbb{Z}/p\mathbb{Z})$ by the previous problem. Determine which of the matrices above is sent to a unit for each choice of $p = 2, 3, 5$.

9. Bases

Let $M = \mathbb{Z}/n\mathbb{Z}$.

(a) Show that M admits no basis as a module over $\mathbb{Z}$.

(b) Show that M admits a basis as a module over the ring $R = \mathbb{Z}/n\mathbb{Z}$.

10. Ideals are like normal subgroups

Let R be a commutative ring. Show that $I \subset R$ is an ideal if and only if it is the kernel of some ring homomorphism. (The kernel of a ring homomorphism $R \to S$ is the set of all elements sent to $0 \in S$.)

11. Characteristic

Let F be a field, and $1 \in F$ the multiplicative identity. The *characteristic* of F is the smallest integer n with $n \geq 1$ such that

$$1 + \ldots + 1 = 0$$

where the summation has n terms in it. For instance, the characteristic of $\mathbb{Z}/p\mathbb{Z}$ is p. If F is a field where $1 + \ldots + 1$ never equals 0 (like $\mathbb{R}, \mathbb{Q}, \mathbb{C}$) we say that F has *characteristic zero*.

Prove that any field (finite or not!) must have either characteristic zero, or characteristic p for some prime number p.

(By the way, there are in fact infinite fields of finite characteristic.)

12. Solvability of S_n.

(a) For $n \geq 3$, show that any cycle of length 3 is in A_n.
(b) Show by example that A_n is not abelian for $n \geq 4$.
(c) Assume A_n is simple for $n \geq 5$. (This is a theorem we stated, but never proved.) Explain why S_n is not solvable for any $n \geq 5$.
(d) Show that S_n is solvable for $n \leq 3$. So all that remains is S_4.
(e) Prove that S_4 is solvable. (One way: You can exhibit an abelian subgroup of order 4 in A_4.)

Math 122 Midterm 2 Fall 2014 Solutions

Common mistakes

i. Groups of order pq are *not* always cyclic. Look back on Homework Eight. Also consider the dihedral groups D_{2n} for n an odd prime.

ii. If $H \subset G$ and H is abelian, it is *not* true that H is necessarily normal. Every subgroup of an *abelian* G is normal, but a subgroup's "abelianness" does not inform you of its normalcy. Consider for instance the subgroup $H \subset S_n$ generated by (123). H is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ so is abelian, but is not normal in S_n unless $n = 3$.

iii. Along these lines: Being normal is not some absolute property of a group. For example, any group H is normal inside itself—$H \triangleleft H$. But if H can be realized as a subgroup of G, it is not necessarily true that $H \triangleleft G$! Likewise, homomorphisms do not "preserve normal subgroups" — i.e., a homomorphism $G_1 \to G_2$ need not send a normal subgroup of G_1 to a normal subgroup of G_2. This is true, however, in special cases, and also when the homomorphism is a surjection.

iv. If $G_1 \triangleleft G_2$ and $G_2 \triangleleft G_3$, it is *not* necessarily true that $G_1 \triangleleft G_3$. Consider for instance

$$G_1 = \{1, (12)(34)\}, \qquad G_2 = \{1, (12)(34), (13)(24), (14)(23)\}, \qquad G_3 = A_4.$$

Then G_1 is *not* normal in G_3—try conjugating by (123).

v. The Klein four-group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So you shouldn't say that "the" Klein 4-group is the normal, order 4 subgroup of A_4. Rather, there exists a subgroup of A_4 isomorphic to the Klein 4-group, and this subgroup happens to be normal in A_4.

vi. For a commutative ring R, the notation $R^\times$ is *not* equal to $R - \{0\}$. Though we haven't used this notation much, $R^\times$ is the notation for the *units* of R. So if R isn't a field, $R^\times \neq R - \{0\}$.

vii. Some people wrote $G/\ker\phi = \text{image}\,\phi$. This isn't correct–the two groups are not equal, they are *isomorphic*. Just as when there is a bijection between two sets, it usually does not mean the two sets are equal. As an example—a set of five bananas is not equal to a set of five apples. But the two sets are in bijection.

viii. In the problem about showing G/K is solvable if G is—if $G_0 \subset \ldots \subset G_n$ is a sequence showing G is solvable, the groups G_i/K might not make any sense, because K may not be a subgroup of G_i!

1. Irreducibility

Let F be a field. For any $x \in F$, note that there is a function

$$F[t] \to F,$$

called *evaluation at* x. Explicitly, if $f = a_d t^d + \dots a_1 t + a_0$ is a polynomial, we send f to

$$f(x) = a_d x^d + \dots a_1 x + a_0 \in F.$$

Here, by x^d, we mean of course the element of F obtained by multiplying x with itself d times.

(a) Show that for any $x \in F$, evaluation at x is a ring homomorphism.

If $f(t) = 1$, then $f(x) = 1$. Further, $(f+g)(x) = \sum (a_i + b_i)x^i = \sum a_i x^i + \sum b_i x^i = f(x) + g(x)$. Finally, $fg(x) = \sum_{i+j=k} a_i b_j x^k = (\sum_i a_i x^i)(\sum_j b_j x^j) = f(x)g(x)$.

(b) Show that f can be factored by a linear polynomial if and only if there is some $x \in F$ for which $f(x) = 0$. (Hint: Use the division algorithm and induct on degree.)

We showed this in class. See Lecture 33.

Recall that a polynomial $f(t) \in F[t]$ is *irreducible* if the only polynomials dividing $f(t)$ are degree 0 (i.e., are constants) or have degree equal to f.

(c) If $F = \mathbb{C}$, show that $f(t) = t^2 + 1$ is not irreducible.

The element $x = \sqrt{-1}$ satisfies this polynomial—$f(\sqrt{-1}) = -1 + 1 = 0$. Hence by above, f is not irreducible.

(d) If $F = \mathbb{R}$, show that $f(t) = t^2 + 1$ *is* irreducible. (Hint: If $f(t) = g(t)h(t)$, what can you say about the degrees of g and h? And what does that say about solutions to $f(t)$?)

If f can be factored into non-units, then both g and h in the hint must be degree one polynomials. Hence by (b), there must be some real number such that $x^2 + 1 = 0$. However, for real numbers, x^2 is always non-negative, so this is impossible.

(e) For each of the primes $p = 2, 3, 5, 7$, indicate which of the following polynomials has a solution in $\mathbb{Z}/p\mathbb{Z}$. (You'll need to just compute.)

(a) $t^2 + \overline{1}$ (i.e., which of these finite fields has a square root to -1?)

We can just compute values of x^2 in each field:

$x \backslash p$	2	3	5	7
1	1	1	1	1
2	–	1	4	4
3	–	–	4	2
4	–	–	1	2
5	–	–	–	4
6	–	–	–	1

of these, only $p = 2$ and $p = 5$ has -1 appearing: For instance, $2^2 = 3^2 = 4 = -1 \in \mathbb{Z}/5\mathbb{Z}$. Explicitly, one can also factor the polynomial as below:

$$t^2 + 1 = (t + 1)(t + 1)$$

in $\mathbb{Z}/2\mathbb{Z}$, and

$$t^2 + 1 = (t - 3)(t - 2)$$

in $\mathbb{Z}/5\mathbb{Z}$.

(b) $t^3 - \overline{2}$ (i.e., which of these fields has a cube root to 2?)
We can just compute values of x^3 in each field:

$x \backslash p$	2	3	5	7
1	1	1	1	1
2	–	2	3	1
3	–	–	2	6
4	–	–	4	1
5	–	–	–	6
6	–	–	–	6

of these, only $p = 3$ and $p = 5$ has 2 appearing: Namely, $2^3 = 3^2 = 4 = -1 \in \mathbb{Z}/5\mathbb{Z}$. Also note that $t^3 - 2$ factors in $\mathbb{Z}/2\mathbb{Z}$, since $x = 0$ is a root. Explicitly, we have the following factorizations:

$$t^3 - 2 = t^3 = t \cdot t \cdot t \qquad \text{in } \mathbb{Z}/2\mathbb{Z}.$$

$$t^3 - 2 = (t - 2)(t^2 + 2t + 1) = (t + 1)^3 \qquad \text{in } \mathbb{Z}/3\mathbb{Z}.$$

$$t^3 - 2 = (t - 3)(t^2 + 3t + 4) \qquad \text{in } \mathbb{Z}/5\mathbb{Z}.$$

(c) t^2+t+1 (i.e., for which of these fields does this polynomial factor?)
We can just compute values of $x^2 + x + 1$ in each field:

$x \backslash p$	2	3	5	7
1	1	0	3	3
2	–	1	2	0
3	–	–	3	6
4	–	–	1	0
5	–	–	–	3
6	–	–	–	1

of these, only $p = 3$ and $p = 7$ has 0 appearing. We have explicit factorizations:

$$t^2 + t + 1 = (t - 1)^2 \qquad \text{in } \mathbb{Z}/3\mathbb{Z}.$$

$$t^2 + t + 1 = (t - 2)(t - 4) \qquad \text{in } \mathbb{Z}/7\mathbb{Z}.$$

2. Principal ideal domains

Let R be an integral domain. We call R a *principal ideal domain* if every ideal $I \subset R$ is equal to (x) for some $x \in R$. That is, every ideal is generated by a single element.

(a) Show that $\mathbb{Z}$ is a principal ideal domain. (We've done this in class, so you can do it, too!)

See class notes. Any subgroup of $\mathbb{Z}$ is equal to $(n) = n\mathbb{Z}$, so in particular, any ideal must also be generated by some single element N.

(b) Let F be a field. Show that $F[t]$ is a principal ideal domain. (Hint: If $I \neq (0)$, let n be the least degree for which a degree n polynomial is in I. If $p(t)$ and $q(t)$ are both degree n polynomials, how are they related? Finally, given any $f(t) \in I$, what happens when you divide $f(t)$ by $p(t)$ and look at the remainder?)

Following the hint: Let n be the smallest degree among non-zero elements in I. Let $p(t)$ be a polynomial in I of degree n. If you divide any $f(t) \in I$ by $p(t)$, the division algorithm tells us that we end up with polynomial of degree less than n—but then we have that

$$f(t) = p(t) \cdot g(t) + r(t), \qquad \deg r(t) < n$$

while

$$r(t) = f(t) - p(t)g(t)$$

must be in I by definition of ideal. This means that $r(t)$ must be zero, or that every polynomial $f(t) \in I$ is divisible by p. Hence $I = (p(t))$. (The hint about $p(t)$ and $q(t)$ to be equal-degree polynomials was unnecessary.)

3. The second isomorphism theorem

Fix a group G. Let $S \subset G$ be a subgroup, and $N \triangleleft G$ be a normal subgroup.

(a) Let SN be the set of all elements in G of the form sx where $s \in S$ and $x \in N$. Show this is a subgroup of G.

Given $s_1, s_2 \in S$ and $x_1, x_2 \in N$, we have that

$$s_1 x_1 s_2 x_2 = s_1 s_2 s_2^{-1} x_1 s_2 x_2 = s_1 s_2 x' x_2$$

for some $x' \in N$ (since N is normal). And $s_1 s_2 \in S$ and $x' x_2 \in N$ since both are closed under multiplication. The identity is in SN since $1 \in S, N$ and $1 \cdot 1 = 1$. Finally, SN contains inverses because

$$x^{-1} s^{-1} = (s^{-1} x' s) s^{-1} = s^{-1} x'$$

where $x' \in N$ is the element such that $x' = s x^{-1} s^{-1}$.

(b) Show that N is a normal subgroup of SN.

We know $gxg^{-1} \in N$ for every $g \in G$ and $x \in N$. Since $SN \subset G$, we in particular have that $gxg^{-1} \in N$ for any $g \in SN$.

(c) Show that $S \cap N$ is a normal subgroup of S.

If $x \in S \cap N$, then for all $s \in S$, we know $sxs^{-1} \in N$ since N is normal in G. On the other hand, S is closed under multiplication, so $sxs^{-1} \in S$ as well. This shows $sxs^{-1} \in N \cap S$.

(d) Exhibit an isomorphism between $S/(S \cap N)$ and SN/N. (Hint: Does the equivalence class $[s]$ in the former group define an equivalence class $[sn]$ in the latter group? Does the n in $[sn]$ matter?)

A solution without using the hint: Consider the composition of homomorphisms

$$S \to SN \to SN/N$$

where the latter is the quotient map, and the former is simply the inclusion (note that $S \subset SN$). This composition is a surjection since for any $n \in N$, the element $[sn] \in SN/N$ is equal to the element $[s] \in SN/N$. Its kernel is the set of those elements s which are in N—i.e., $S \cap N$. So we are finished by the first isomorphism theorem.

Alternative proof: This is an explicit construction of the inverse map—illustrated here in case you wanted something more hands-on. Given $[sn] \in SN/N$, consider $[s] \in S/(S \cap N)$.

- We claim the assignment $\phi : [sn] \mapsto [s]$ is well-defined. For if $sn = s'n'x$ with $x \in N$, then

$$s = s'(n'xn^{-1}).$$

We must show that the element $n'xn^{-1}$ is in $S \cap N$. Well, we see it must be in S by multiplying both sides on the left by s'^{-1}. We

know that it's in N since the elements n', x, n^{-1} are all in N and N is closed under multiplication.

- Now we show it is a group homomorphism:

$$\begin{aligned}\phi([s_1n_1][s_2n_2]) = \phi([s_1n_1s_2n_2)] &= \phi([s_1s_2(s_2^{-1}n_1s_2n_2)]) \\ &= \phi([s_1s_2(n'n_2)]) \\ &= [s_1s_2] \\ &= [s_1][s_2] \\ &= \phi([s_1n_1])\phi([s_2n_2]).\end{aligned}$$

- To show it is an injection, we must show that the kernel is trivial. Well, if $\phi([sn]) = [x]$ for $x \in S \cap N$, then $[sn]$ has a representative of the form xn'; but $x \in X \cap N, n' \in N$ implies $xn' \in N$ by the fact that N is closed under multiplication, so $[sn] = [sn'] = 1 \in SN/N$.
- To show surjection, note that for any $s \in S$, we have that $s = s1_G \in SN$. So $\phi([s1_G]) = \phi(s)$.

4. Subgroups descend to quotient groups

Let G be an arbitrary group, and $H \triangleleft G$.

(a) Show that there is a bijection between the set of subgroups in G containing H, and the set of subgroups in G/H.

Let $p : G \to G/H$ be the group homomorphism given by sending $g \mapsto [g]$.

- Given a subgroup $K \subset G$, note the composition of group homomorphisms
$$K \hookrightarrow G \to G/H.$$
Since the image of any group homomorphism is a subgroup, this shows that $p(K)$ is a subgroup of G/H. So we have a function $\{\text{subgroups of } G\} \to \{\text{subgroups of } G/H\}$ given by sending $K \mapsto p(K)$.
- We show it is a surjection: Given $K' \subset G/H$, consider the preimage $p^{-1}(K') \subset G$. This is a subgroup of G since if $p(x), p(y) \in K'$, then $p(xy) = p(x)p(y) \in K'$ (because K' is closed under multiplication).
- Now it suffices to show that $p^{-1}(p(K)) = K$ for all subgroups $K \subset G$. Obviously $K \subset p^{-1}(p(K))$. To show the other inclusion, let $x \in p^{-1}(p(K))$. We know by definition of $p(K)$ that there is some $y \in K$ for which $p(x) = p(y)$. Then $p(xy^{-1}) = 1_{G/H}$, so $xy^{-1} \in H$. Since K contains H, $xy^{-1} \in K$, hence $x \in K$.

(b) Show that there is a bijection between the set of *normal* subgroups in G containing H, and the set of normal subgroups in G/H. (This time, this isn't extra credit.)

- We show that if K is normal, then $p(K)$ is normal. (This proves we have a function

$\{\text{normal subgroups of } G\} \to \{\text{normal subgroups of } G/H\}$.)

Well, if $[k] \in p(K)$, then $[g][k][g]^{-1} = [gkg^{-1}] = [k']$ for some $k' \in K$ since K is normal in G. So $p(K) \subset G/H$ is normal. (Note we are using the fact that $G \to G/H$ is a surjection here—otherwise, we wouldn't know that every element of G/H is in the image of $p(G)$.)
- Surjectivity: We show that if $p(K)$ is normal, then $K = p^{-1}(p(K))$ is normal (this equality follows from part (c) above). If $k \in K$ and $g \in G$, we have that $[gkg^{-1}] = [g][k][g^{-1}] = [k']$ for some $[k'] \in p(K)$—i.e., for some $k' \in K$. So $gkg^{-1} \in p^{-1}(p(K)) = K$.
- We know that this assignment is an injection by part (c) from the previous problem's solution. So we are finished.

5. Solvable groups

A group G is called *solvable* if there exists a finite sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian.

(a) Show that any abelian group is solvable. (If this seems trivial, it's because it is.)

If G is abelian, take $G_0 = 1$ and $G_n = G_1 = G$. This shows G is solvable.

(b) Show any group of order pq, where p and q are distinct primes, is solvable.

Assume $p < q$. We know any such group G has a normal subgroup H of order q—hence, a normal subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z}$ (since any group of prime order is cyclic). We know the existence of such a normal subgroup by applying the Sylow theorems—see Lecture 22—or by 5(b) of Homework Five. This guarantees that we have a short exact sequence

$$1 \to H \to G \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

(Note that G/H must have order $|G|/|H_q| = pq/q = p$, so we know it has to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$.) So take

$$1 = G_0 \subset G_1 = H \subset G_2 = G.$$

Then $G_1/G_0 \cong H \cong \mathbb{Z}/q\mathbb{Z}$ is abelian, and $G_2/G_1 \cong \mathbb{Z}/p\mathbb{Z}$ is, too.

(c) Show that if G is simple and non-abelian, G cannot be solvable.

Since G is simple, it has no normal subgroups aside from G and $\{1\}$. So if $G_{i-1} \triangleleft G_i$ with $G_i = G$ and $G_{i-1} \neq G_i$, we must have that $G_{i-1} = \{1\}$. But then $G_i/G_{i-1} \cong G$ is not abelian, so G is not solvable.

The following is a great application of the isomorphism theorems, and of the previous problem.

(d) Show that if G is solvable, so is any subgroup of G.

Let $S \subset G$ be a subgroup. If G is solvable, there is some sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian. So consider the sequence

$$1 = S_0 \subset S_1 \subset \ldots \subset S_n = S, \qquad S_i = S \cap G_i.$$

- We know $S_{i+1} \subset G_{i+1}$ is a subgroup, and $G_i \triangleleft G_{i+1}$, so by 3(c) of this midterm, we conclude that $S_{i+1} \cap G_i = S_i$ is normal in S_{i+1}.

- So we must now show that S_{i+1}/S_i is abelian. Consider the composition
$$S_{i+1} \hookrightarrow G_{i+1} \to G_{i+1}/G_i$$
which we call ϕ. (The first homomorphism is the inclusion, while the second is the quotient homomoprhism.) By definition of the quotient, the kernel of ϕ is the set of all elements in S_{i+1} that are also in G_i—that is, the kernel is S_i. Hence S_{i+1}/S_i is isomorphic to the image of ϕ by the first isomorphism theorem. But any subgroup of any abelian group is abelian, and the image of ϕ is a subgroup of G_{i+1}/G_i—which is abelian by assumption.

(e) Show that if G is solvable, and $K \subset G$ is normal, then G/K is solvable.

Let $p : G \to G/K$ be the quotient homomorphism. Since G is solvable, we can find a sequence of subgroups
$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$
such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian. Consider the sequence
$$1 = H_0/K \subset H_1/K \subset \ldots \subset H_n/K = G/K, \qquad H_i = G_iK,$$
We claim this sequence satisfies the properties necessary to show that G/K is solvable. Note that since K is normal in G and $G_i \triangleleft G_{i+1}$, we see that $H_i \triangleleft H_{i+1}$. (Explicitly: If $X \in G_{i+1}$ and $Y \in K$, with $x \in G_i, y \in K$, we have
$$\begin{aligned}(XY)xy(XY)^{-1} &= XYxyY^{-1}X^{-1} \\ &= Xxx^{-1}Yxy Y^{-1}X^{-1} \\ &= XxY'yY^{-1}X^{-1} \\ &= XxX^{-1}XY'yY^{-1}X^{-1} \\ &= x'X(Y'yY^{-1})X^{-1} \\ &= x'y'.\end{aligned}$$
When we replace Y by Y', or x by x', we are using the normalcy of the subgroup containing Y, or x.) So by 4(b), we know that $H_i/K \triangleleft H_{i+1}/K$. By the third isomorphism theorem, we know
$$(H_{i+1}/K)/(H_i/K) \cong H_{i+1}/H_i$$
but this latter group is $G_{i+1}K/G_iK$. Setting $S = G_{i+1}$ and $N = G_iK$ (which is normal in $G_{i+1}K$), note that $G_{i+1}K = SN$. (This is because $G_i \subset G_{i+1}$.) So the second isomorphism theorem gives us the isomorphism in the following line:
$$G_{i+1}K/G_iK = SN/N \cong S/(S \cap N) = G_{i+1}/(G_{i+1} \cap G_iK).$$

But since $G_i \subset (G_{i+1} \cap G_i K)$, this last group receives a surjective homomorphism

$$G_{i+1}/G_i \to G_{i+1}/(G_{i+1} \cap G_i K).$$

Any group receiving a surjective homomorphism from an abelian group must be an abelian group.

6. $GL_n(\mathbb{F}_q)$

Let $\mathbb{F}_q$ be a finite field with q elements.

(a) Let $V = \mathbb{F}_q^n = \mathbb{F}_q^{\oplus n}$ be an n-dimensional vector space over $\mathbb{F}_q$. Show that $G = GL_n(\mathbb{F}_q)$ acts *transitively* on $V - \{0\}$. (That is, show that for any pair $x, y \in V$, there is some group element g so that $gx = y$.)

Fix x. If we can show that for all y, there exists g so that $gx = y$, we're finished. For given another element x', we are guaranteed an element h so that $hx' = x$. Then

$$(gh)x' = g(hx') = gx = y.$$

So let x be the standard column vector

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

If y is any non-zero vector, note that it alone forms a linearly independent set. But any linearly independent collection of vectors can be completed to a basis (29.18 from Lecture 29)—so let $y_1, y_2, \ldots, y_n$ be some basis where $y_1 = y$. Then the matrix g whose ith column is y_i is invertible. (Page 3, Lecture 36.) Moreover, by definition of matrix multiplication, $gx = y_1 = y$.

- - - -For an alternative proof: If y is a column vector whose top entry is $y_1 \neq 0$, then the matrix g whose first column is given by y, and is otherwise a diagonal matrix with 1 along the diagonal:

$$g = \begin{bmatrix} y_1 & 0 & 0 & \ldots & 0 \\ y_2 & 1 & 0 & \ldots & 0 \\ y_3 & 0 & 1 & \ldots & 0 \\ \vdots & \ldots & \ldots & \ldots & \vdots \\ y_n & 0 & 0 & \ldots & 1 \end{bmatrix}$$

This is invertible since its determinant is $y_1 \neq 0$, and satisfies $gx = y$. On the other hand, if $y_1 = 0$, there is some entry of y with $y_i \neq 0$ since $y \neq 0$. In this case, let g' be the matrix whose ith column is y, and which is otherwise a diagonal matrix with 1 along the diagonal. This is invertible because its determinant is $y_i \neq 0$. Also consider the matrix h which swaps the ith standard basis vector with the 1st, and leaves all other standard basis vectors intact. (This is the matrix corresponding to the permutation (1i).) Then we have that $(gh)x = y$.

- - - - For another proof: Some people wanted to show that if x_i form a basis and y_i form a basis, there is some invertible transformation A

taking $x_i \mapsto y_i$. (This is overkill, but yields the result we need: Given x and y, complete each of them to a basis, and use the matrix A.) So let's prove the claim. Well, by definition, a basis $x_1, \ldots, x_n$ determines an $\mathbb{F}$-module isomorphism

$$T_x : \mathbb{F}^n \to \mathbb{F}^n, \qquad e_i \mapsto x_i$$

where e_i are the standard basis vectors. Likewise, the basis $y_1, \ldots, y_n$ determines an $\mathbb{F}$-module isomorphism

$$T_y : \mathbb{F}^n \to \mathbb{F}^n, \qquad e_i \mapsto y_i.$$

You can check that the inverse of an $\mathbb{F}$-module homomorphism is again an $\mathbb{F}$-module homomorphism, and that the composition of invertible $\mathbb{F}$-module homomorphisms is again invertible. So consider

$$A = T_y \circ (T_x)^{-1}.$$

This is an invertible transformation that takes y_i to x_i by definition.

(b) Prove that $G = GL_n(\mathbb{F}_q)$ has

$$\left(\prod_{k=1}^{n}(q^k - 1)\right)\left(\prod_{k=1}^{n-1} q^k\right)$$

elements in it. (You can either count intelligently, or apply the orbit-stabilizer theorem inductively. Either way, use matrices.)

First note that if $n = 1$, we have that $GL_1(\mathbb{F}_q)$ is the set of invertible 1×1 matrices—that is, the set of all invertible elements in $\mathbb{F}_q$. Since $\mathbb{F}_q$ is a field, this means that $|GL_1(\mathbb{F}_q)| = q - 1$.

Now: Let $x = e_1$ be the standard basis vector with 1 in the first entry and 0 elsewhere. The stabilizer of x is the set of all matrices g for which $gx = x$—that is, the set of all matrices whose first column is given by e_1. (This is because ge_1 always equals the first column of g—if you're not sure why, try writing it out.) How many such invertible matrices are there? Well, writing

$$g = \begin{bmatrix} 1 & -\vec{u}- \\ 0 & A \end{bmatrix}$$

where $\vec{u}$ is some row vector with $n-1$ entries, and A is a $(n-1)\times(n-1)$ matrix, we see that $\det g = \det A$. So g is invertible if and only if A is, while the entries of $\vec{u}$ have no effect on whether g is invertible. By the orbit stabilizer theorem,

$$|GL_n(\mathbb{F}_q) = |\mathcal{O}_x| \cdot |\text{Stabilizer}(x)|.$$

By above, the orbit of x is all of $\mathbb{F}_q^n - \{0\}$—but $\mathbb{F}_q^n$ has q^n elements in it, so removing $\{0\}$ yields an orbit with size $q^n - 1$. On the other hand, an element of the stabilizer is determined uniquely by a choice

of A and of $\vec{u}$—there are $|GL_{n-1}(\mathbb{F}_q)|$ choices for A, and q^{n-1} choices for $\vec{u}$. Thus we have that

$$|GL_n(\mathbb{F}_q)| = (q^n - 1) \cdot (q^{n-1})(|GL_{n-1}(\mathbb{F}_q)|).$$

Now you can check that the formula holds as claimed, by induction.

(c) Show that $GL_n(\mathbb{F}_q)$ has a normal subgroup of index $q-1$. (Hint: The determinant is still a group homomorphism.)

The group homomorphism $GL_n(\mathbb{F}_q) \to (\mathbb{F}_q - \{0\})$ is a surjection. (For instance, take the diagonal matrix with diagonal entries given by 1 and by a single appearance of a. This has determinant a.) Hence the index of its kernel is given by the size of the target group, which is $q-1$.

(d) Consider $G = GL_2(\mathbb{F}_q)$. Assume p is the unique prime number dividing q. [1] Show that $|\operatorname{Syl}_p(G)|$ cannot equal 1. (Try thinking about upper-triangular and lower-triangular matrices, then think about special cases of them.)

The group $GL_2(\mathbb{F}_q)$ has size

$$(q^2 - 1)(q - 1)q$$

according to the previous problem. So any subgroup of size q is a Sylow p-subgroup. (If q is divisible by only p, then no number of the form $q^k - 1$ is divisible by p.) We claim that the set of all upper-triangular matrices with 1 along the diagonal, and the set of all lower-triangular matrices with 1 along the diagonal, each form a subgroup of order q—thus $\operatorname{Syl}_p(\mathbb{F}_q)$ has more than one element.

- - - Note that the size of each set is obviously q. The determinant of an element in either of these sets is 1, and the identity matrix is in both sets, so we just need to prove that both are closed under multiplication:

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

The proof for the lower-triangular case is identical; just take the transpose of each matrix.

- - - - By the way, you can show that for any n, the upper-triangular matrices with 1 along the diagonal constitute a q-Sylow subgroup of $GL_n(\mathbb{F}_q)$.

- - - - - Another proof, even without producing a Sylow subgroup: Note that the sizes of the set of upper-triangular and lower-triangular matrices are divisible by q, so these must contain p-Sylow subgroups, H and

[1] One can prove that any finite field has size p^k for some prime p.

As pointed out to me by Kevin, it's not hard—a finite field of characteristic p is a module over $\mathbb{Z}/p\mathbb{Z}$, so is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. But how many elements must such a set have?

K. But the intersection of the upper-triangular and lower-triangular matrices are the diagonal matrices, of which there are $(q-1)^n$ (a number not divisible by q). Hence the p-Sylow subgroups contained in H and K must be distinct.

(e) How many elements of order 3 are in $GL_2(\mathbb{F}_3)$? (You may want to start by determining the number of Sylow 3-subgroups. Either way, dig in.)

Note that the 3-Sylow subgroups of $GL_2(\mathbb{F}_3)$ are given by subgroups of order 3. Note also that if two subgroups of order 3 have an intersection that contains more than the identity, then the two subgroups must be equal (you can check this). Moreover, for each distinct 3-Sylow subgroup H, the generator $x \in H$ and its square, x^2, represent distinct elements of order 3. Conversely, any element of order 3 determines a 3-Sylow subgroup by looking at the subgroup it generates. Hence the number of elements of order 3 is given by $2 \cdot |\operatorname{Syl}_3(GL_2(\mathbb{F}_3))|$.
- - - - By (d), we know that $s := |\operatorname{Syl}_3(GL_2(\mathbb{F}_3))| \geq 2$. By the Sylow theorems, the number s must divide

$$(q^2-1)(q-1) = 8 \cdot 2 = 16$$

and must equal 1 modulo 3. This leaves the options of $s = 4$ or $s = 16$. Claim: $s = 16$ is impossible. Note that then we would have $2 \cdot 16 = 32$ elements of order 3. And the Sylow Theorem guarantees that we have at least one group of order 16—the 2-Sylow subgroup. Since $32 + 16 = 48 = |GL_2(\mathbb{F}_3)|$, this implies there can be no elements of order other than 3 (those elements in a subgroup of order 3), or some power of 2 (those elements in the Sylow 2-subgroup). But there is in fact an element of order 6 in $GL_2(\mathbb{F}_3)$, given by

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

To see this, note

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

while

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & an \\ 0 & 1 \end{bmatrix}$$

in general. So $s = 16$ leads to a contradiction, and we conclude that $s = 4$. this means that there are $2 \cdot 4 = 8$ elements of order 3.
- - - - Another proof that $s = 16$ is impossible: Any element of order 3 must have determinant 1—after all, $(\det g)^3 = \det g^3 = \det I = 1$, and the only cube root of 1 in $\mathbb{F}_3$ is 1. But the kernel of the determinant has $|GL_2(\mathbb{F}_3)|/|\mathbb{F}_3 = \{0\}| = 48/2 = 24$ elements in it, so it couldn't contain 32 elements.

- - - - Yet another proof that $s = 16$ is impossible: From the proof of the Sylow theorems, we know that $[GL_2(\mathbb{F}_3) : N(H)] = s$, where $N(H)$ is the normalizer of the Sylow 3-subgroup H. But the elements

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

all normalize the 3-Sylow subgroup H of upper triangular matrices with 1 along the diagonal. Hence $|N(H)| \geq 4$, and s must be less than 16.
- - - - - Another proof: Let K be the kernel of the determinant map. It's a normal subgroup of index 2, so of order 24. By Sylow's theorems, you can see that K must contain either 1 or 4 subgroups of order 3 (check this yourself). But the upper and lower-triangular matrices with 1 along the diagonal are both subgroups of K, so there must be 4 subgroups of order 3 in K. Since any 3-Sylow subgroup of $GL_2(\mathbb{F}_q)$ must be conjugate by Sylow's theorems, they must all be contained in K since K is closed under conjugation. So these 4 subgroups in K are also all the 3-Sylow subgroups of $GL_2(\mathbb{F}_q)$, and we have that $s = 4$.

No more collaboration

7. Ring homomorphisms

(a) Show that a composition of two ring homomorphisms is a ring homomorphism.

Let $f : R \to S$ and $g : S \to T$ be ring homomorphisms. We know the composition of two group homomorphisms is a group homomorphism, we know that $g \circ f$ is a group homomorphism under addition. Thus we need only check that $g \circ f(r_1 r_2) = (g \circ f(r_1))(g \circ f(r_2))$, and that $g \circ f(1_R) = 1_T$. The first equality follows because

$$g \circ f(r_1 r_2) = g(f(r_1)f(r_2)) = g(f(r_1))g(f(r_2)).$$

The last follows because $gf(1_R) = g(1_S) = 1_T$.

(b) For a ring R, let $M_{k\times k}(R)$ denote the ring of $k \times k$ matrices with entries in R. Specifically, if (a_{ij}) is a matrix whose i, jth entry is a_{ij}, we define

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \qquad (a_{ij})(b_{ij}) = (\sum_{l=l}^{k} a_{il} b_{lj}).$$

Show that if $f : R \to S$ is a ring homomorphism, then the function

$$F : M_{k\times k}(R) \to M_{k\times k}(S), \qquad (a_{ij}) \mapsto (f(a_{ij}))$$

is a ring homomorphism.

To show that F is a group homomorphism with respect to addition, let a_{ij} and bij be the i, jth entries of matrices A, B having entries in R. Then

$$F(A + B)_{ij} = f(a_{ij} + b_{ij}) = f(a_{ij}) + f(b_{ij}) = (F(A) + F(B))_{ij}.$$

Since the i, jth entries of both matrices agree, we have that $F(A+B) = F(A) + F(B)$. To show that the multiplicative identity is mapped to the multiplicative identity, note that the identity of the ring of $k \times k$ matrices is given by the diagonal matrix with diagonal entries 1_R and 1_S, respectively. But since f is a ring homomorphism, F sends the identity of $M_{k\times k}(R)$ to that of $M_{k\times k}(S)$. Finally, we must show that F respects multiplication. To see this, note

$$F(AB)_{ij} = f(\sum_{l=1}^{k} a_{il} b_{lj}) = \sum_{l=1}^{k} f(a_{il}) f(b_{lj}) = \sum_{l=1}^{k} F(A)_{il} F(B)_{lj} = (F(A)F(B))_{ij}.$$

(c) Prove that

$$f(\det A) = \det(F(A)).$$

You may want to start by proving it for $k = 1$, then perform induction using the cofactor definition of determinants.

This is true for $k = 1$, since a 1×1 matrix A is the data of choice of an element $a \in R$, and its determinant is equal to a. Hence

$$f(\det A) = f(a) = \det F(A).$$

By induction, assume the equality holds for matrices of dimension $\leq k - 1$. We have that

$$f(\det A) = f(\sum_{i=1}^{k} (-1)^{i+1} a_{0i} \det C_{0i})$$

where C_{0i} is the matrix obtained by deleting the 0th row and ith column of A. Since f is a ring homomorphism, we have that this in turn equals

$$\sum_{i=1}^{k} (-1)^{i+1} f(a_{0i}) f(\det C_{0i}) = \sum_{i=1}^{k} (-1)^{i+1} F(A)_{0i} \det F(C_{0i}).$$

Noting that $F(C_{0i})$ is the cofactor matrix of $F(A)$ given by deleting the 0th row and ith column, we are finished.

8. Invertible matrices

Let S be a ring. We say $x \in S$ is a *unit* if there is a multiplicative inverse to x—i.e., an element $y \in S$ so that $xy = yx = 1_S$. As an example, if S is the ring of $k \times k$ matrices in some ring R, then a matrix is invertible if and only if it is a unit.

(a) Determine which of the following matrices is a unit in $M_{k\times k}(\mathbb{Z})$:

$$\begin{pmatrix} 2 & 5 \\ 4 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix}$$

None of them. A matrix with coefficients in R is a unit if and only if its determinant is a unit in R. But the determinant of the above three matrices are

$$8 - 20 = 12, \qquad 8 - 45 = -37, \qquad 21 - 24 = 3$$

respectively. However, the only units in $\mathbb{Z}$ are ± 1.

(b) For the primes $p = 2, 3, 5$, consider the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ sending $a \mapsto \overline{a}$. This induces a ring homomorphism $M_{k\times k}(\mathbb{Z}) \to M_{k\times k}(\mathbb{Z}/p\mathbb{Z})$ by the previous problem. Determine which of the matrices above is sent to a unit for each choice of $p = 2, 3, 5$.

Modulo p, the integer determinants $12, -37, 3$ above are given respectively by

$$\begin{aligned} &0, \quad 1, \quad 1 \quad (mod 2) \\ &0, \quad 2, \quad 0 \quad (mod 3) \\ &2, \quad 3, \quad 3 \quad (mod 5). \end{aligned}$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the invertible matrices are those who determinants are non-zero, (since, in a field, any non-zero element is a unit).

9. Bases

Let $M = \mathbb{Z}/n\mathbb{Z}$.

(a) Show that M admits no basis as a module over $\mathbb{Z}$.

The easiest proof: Any basis induces an isomorphism $\mathbb{Z}^k \to M$. But M is finite, while $\mathbb{Z}^k$ is finite if and only if $k = 0$.
- - - - A more hands-on proof: For any element $x \in M$, we have that $nx = 0 \in M$. Hence M does not admit any non-empty sets of linearly independent elements, hence admits no basis.

(b) Show that M admits a basis as a module over the ring $R = \mathbb{Z}/n\mathbb{Z}$.

Let $x = \overline{1}$. This is a spanning set because for any $\overline{j} \in M$, we know that $\overline{j} = \overline{j} \cdot x$. It is linearly independent because $\overline{a}x = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ means that $a \cdot 1$ is a multiple of n. But this means a itself must be a multiple of n, hence $\overline{a} = \overline{0} \in R$.

10. Ideals are like normal subgroups

Let R be a commutative ring. Show that $I \subset R$ is an ideal if and only if it is the kernel of some ring homomorphism. (The kernel of a ring homomorphism $R \to S$ is the set of all elements sent to $0 \in S$.)

Let $\phi : R \to S$ be a ring homomorphism. If $x \in \ker \phi$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0_S = 0_S.$$

So $\ker \phi$ is closed under scaling by arbitrary elements of R. Likewise, the kernel of a ring homomorphism is by definition the kernel of the group homomorphism $\phi : (R, +) \to (S, +)$ so it is a subgroup of R under addition. This proves $\ker(\phi)$ is an ideal. For the converse, we know that any ideal $I \subset R$ of a commutative ring defines a ring homomorphism $R \to R/I$ given by $r \mapsto \overline{r}$. The kernel is precisely those elements in I, so any ideal is a kernel of a ring homomorphism.

11. Characteristic

Let F be a field, and $1 \in F$ the multiplicative identity. The *characteristic* of F is the smallest integer n with $n \geq 1$ such that

$$1 + \ldots + 1 = 0$$

where the summation has n terms in it. For instance, the characteristic of $\mathbb{Z}/p\mathbb{Z}$ is p. If F is a field where $1 + \ldots + 1$ never equals 0 (like $\mathbb{R}, \mathbb{Q}, \mathbb{C}$) we say that F has *characteristic zero*.

Prove that any field (finite or not!) must have either characteristic zero, or characteristic p for some prime number p.

(By the way, there are in fact infinite fields of finite characteristic.)

We first note that n cannot equal 1. If so, we have that $1 = 0$. But then $F - \{0\}$ cannot be a group with F being a ring. To see this, let $e \in F - \{0\}$ be the identity. Then $ex = x$ for all $x \neq 0$, and $e0 = 0$ so e is also the multiplicative unit of F—the contradiction arises by the uniqueness of the multiplicative unit of F, which demands that $e = 1$. So n cannot be 1.
- - - -Clearly $1 + \ldots + 1 = 0$ for some finite summation with n terms in it, assume that n is divisible by two numbers, ab, neither of which is 1. Then we have that

$$(1 + \ldots + 1)(1 + \ldots + 1) = 0$$

where the left factor has a summands, and the right factor has b summands. But since F is a field, if two elements multiply to 0, one of them must equal zero. (As we proved in class, units are not zero divisors, and every non-zero element of a field is a unit.) But then a summation of either a or b terms of 1 equals zero, contradicting the assumption that n is the smallest such number. Hence either a or b must equal 1, meaning n must be prime.

12. Solvability of S_n.

(a) For $n \geq 3$, show that any cycle of length 3 is in A_n.

Let (ijk) be a cycle of length three. It is a composition $(ij) \circ (jk)$, but the sign of (ij) is minus one. Since the sign map from $S_n \to \{\pm 1\}$ is a homomorphism, this means that the sign of $(ij) \circ (jk)$ is given by $-1 \times -1 = 1$; hence (ijk) is in the kernel of the sign map.

(b) Show by example that A_n is not abelian for $n \geq 4$.

Consider the cycles (123) and (234). We have

$$(123) \circ (234) = (21)(34), \qquad (234) \circ (123) = (13)(24)$$

so these two elements of A_n, $n \geq 4$ do not commute.

(c) Assume A_n is simple for $n \geq 5$. (This is a theorem we stated, but never proved.) Explain why S_n is not solvable for any $n \geq 5$.

By 5(c), a non-abelian, simple group is not solvable. So A_n is not solvable for $n \geq 5$. If S_n is solvable, so would any subgroup of it be (by 5(d)), so S_n is not solvable for $n \geq 5$.

(d) Show that S_n is solvable for $n \leq 3$. So all that remains is S_4.

If $n = 1$, S_1 is the trivial group, so one can take $G_0 = G_n$ and we have that S_1 is solvable. $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ so it is solvable, being abelian, by 5(a). Finally, S_3 has order 6, which is solvable by 5(b).

(e) Prove that S_4 is solvable. (One way: You can exhibit an abelian subgroup of order 4 in A_4.)

Suppose there is an abelian, normal subgroup H of order 4 in A_4. Then A_4/H must be a group of order $12/4 = 3$, hence a cyclic (and abelian) group. Then the sequence

$$1 = G_0 \subset G_1 = H \subset G_2 = A_4 \subset G_3 = S_4$$

would show that S_4 is solvable. (Note $G_3/G_2 \cong \mathbb{Z}/2\mathbb{Z}$.) Let

$$H = \{1, a = (12)(34), b = (13)(24), c = (14)(23)\}.$$

Note each element is its own inverse so H is closed under taking inverses. To see it is closed under multiplication, first note

$$(12)(34) \circ (13)(24) = (14)(23), \qquad (13)(24) \circ (12)(34) = (14)(23).$$

Since each of these elements is their own inverse, we see that $ab = c, ba = c$ implies $a = cb = bc$ and $b = ac = ca$; hence this set is abelian and closed under multiplication. (It's in fact isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, though we don't need that.) Finally, to conclude that H is closed under conjugation, recall that in the symmetric group, conjugation preserves cycle shape. And every element whose cycle shape is given by two disjoint cycles of length 2 is in H—so in fact, H is a normal subgroup of S_4. This implies it's a normal subgroup of A_4.

Math 122 Fall 2014 Practice Problems for Final

Practice Problems for matrices and Cayley-Hamilton

1. Basics in characteristic polynomials

(a) Let F be a field, and A a $k \times k$ matrix with entries in F. Show that A is not conjugate to an upper-triangular matrix unless its characteristic polynomial can be factored into (possibly non-distinct) linear polynomials in $F[t]$.
(b) Given an example of a matrix in a field F whose characteristic polynomial cannot be factored into linear polynomials.
(c) Prove that if A is a $k \times k$ matrix with entries in a field F, its characteristic polynomial $\Delta(t)$ is a degree k polynomial in $F[t]$, and that the degree $k-1$ coefficient of $\Delta(t)$ is $-\mathrm{tr}(A)$. (Here, $\mathrm{tr}(A)$ is the trace of A—the sum of its diagonal entries.)
(d) Prove that the constant term of $\Delta(t)$ is $(-1)^k \det A$.

2. Matrices are linear transformations

Let R be a commutative ring and $R^{\oplus k}$ the free module on k generators. Show there is a ring isomorphism

$$T : M_{k\times k}(R) \to \hom_R(R^{\oplus k}, R^{\oplus k})$$

given by sending a matrix A to the homomorphism T_A sending the ith standard basis element of $R^{\oplus k}$ to the element

$$\sum_{j=1}^{k} A_{ji} e_j.$$

If you are lazy and don't want to do every part of the proof, here is the most important part: prove that $T_{AB} = T_A \circ T_B$, so that matrix multiplication is sent to composition of functions.

Remark 2.1. (Recall that a homomorphism from $R^{\oplus k}$ to any module M is determined by the choice of k elements $x_1, \ldots, x_k$ in M, simply be declaring that $e_i \in R^{\oplus k}$ get sent to x_i.)

Remark 2.2. To be clear, the target of T is the set of all left R-module homomorphisms from $R^{\oplus k}$ to itself.

Remark 2.3. By the way, this ring isomorphism is the justification for saying that a linear map from a finite-dimensional vector space over F to itself is the same thing as a matrix—in this case, $R = F$, and every finite-dimensional vector space over F is isomorphic to $F^{\oplus k}$ for some k.

3. Some Cayley-Hamilton applications

Let $\mathbb{F}$ be a field of characteristic p. Let A be an upper-triangular $k \times k$ matrix with entries in $\mathbb{F}$.

(a) Assume A's diagonal entries are equal to 1. Show that for the values $(3,3)$, $(5,5)$, and $(4,2)$ of (k,p), A^k is equal to $(-1)^{k-1}I$.
(b) With the hypothesis as in part (a), prove that A is an element whose order must divide k or $2k$.

4. More Cayley-Hamilton

Let F be a field and A an $k \times k$ matrix with entries in F. When you want to compute $f(A)$ where $f(t)$ is some high-degree polynomial in t, note that by the division algorithm for polynomials, we can write

$$f(t) = q(t)\Delta(t) + r(t)$$

where $\Delta(t)$ is the characteristic polynomial of A. Then we have

$$f(A) = q(A)\Delta(A) + r(A) = r(A)$$

since $\Delta(A) = 0$ by the Cayley-Hamilton theorem. This reduces a potential costly calculation into two steps: A division of polynomials (to find r) and then a degree $k-1$ computation given by evaluating $r(A)$.

(a) If A is a 2×2 matrix which is not invertible in F, prove that A^2 is always a scalar multiple of A. Moreover, prove that A^2 is obtained from A by scaling via the trace of A.
(b) Let A be a 3×3 matrix which is not invertible, and which has trace zero. Compute A^{1000} in terms of A^2 and the degree 1 coefficient of $\Delta(t)$. Derive a general formula for A^N in terms of A^2 and the degree 2 coefficient of $\Delta(t)$.
(c) Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 5 & 2 & -1 \end{bmatrix}.$$

Compute A^{2014} using the methods above.
(d) What is A^{2014} if you consider A as a matrix with entries in $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$?

Rings and ideals

5. Basics of rings

(a) Give an example of a non-commutative ring with a zero divisor. (Make sure to identify the zero divisor.)
(b) Given an example of a commutative ring with a zero divisor.

6. Prime ideals

Let R be a commutative ring. An ideal I is called *prime* if whenever $xy \in I$, we have that either $x \in I$ or $y \in I$.

(a) Let $f \in R$ be an irreducible element and R a PID. Show that the ideal generated by f is prime.
(b) Recall that a commutative ring is called a *domain* if it has no zero divisors. Show that if I is a prime ideal of R, then R/I is a domain.

7. Prime ideals and maximal ideals

Let R be a commutative ring.

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

8. A ring that is not a PID

(a) Let F be a field, and let $R = F[x_1, x_2]$ be the ring of polynomials with two variables. Exhibit an ideal in R that is not principal.
(b) Show that $\mathbb{Z}[x]$—the ring of polynomials with $\mathbb{Z}$ coefficients—is not a principal ideal domain.

Modules

9. $\mathbb{Z}$-modules

(a) Show that a $\mathbb{Z}$-module is the same thing as an abelian group.
(b) Show that a map of $\mathbb{Z}$-modules (i.e., a $\mathbb{Z}$-linear homomorphism between $\mathbb{Z}$-modules) is the same thing as a homomorphism of abelian groups.

10. $\mathbb{Z}[t]$-modules

Show that a $\mathbb{Z}[t]$-module structure on an abelian group M is the same thing as giving an abelian group homomorphism from M to itself.

11. Submodules

Let M be a left R-module. Recall that an *R-submodule* of M is a subgroup $N \subset M$ such that $rx \in N$ for all $r \in R, x \in N$.

(a) Show that the intersection of two submodules is a submodule.
(b) If R is a commutative ring and $R = M$, show that a submodule of M is the same thing as an ideal of R.

12. Not all modules are free

Give an example of a ring R and a left module M such that M is not isomorphic to a free R-module.

Computations

13. Computations with matrices

Consider the matrices

$$\begin{bmatrix} 1 & 4 \\ 5 & 7 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}.$$

(a) Which of them are invertible as elements of $M_{2\times 2}(\mathbb{Z})$?
(b) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$?
(c) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$?

14. Polynomial roots

Consider the polynomials

$$t^3 + 2t + 1, \qquad t^4 + 1, \qquad t^2 + 3.$$

(a) Which of these are irreducible elements of $\mathbb{Z}/2\mathbb{Z}[t]$?
(b) Which of these are irreducible elements of $\mathbb{Z}/3\mathbb{Z}[t]$?
(c) Which of these are irreducible elements of $\mathbb{Z}/5\mathbb{Z}[t]$?

Classification of finitely generated PIDs

15. Statement

State the classification of finitely generated modules over a PID.

16. Classifying abelian groups

(a) How does the theorem let us classify finitely generated abelian groups?
(b) Classify all abelian groups of order 12.
(c) Classify all abelian groups of order 16.

17. Another way to phrase classification of abelian groups

(a) Let k, m, n be integers. Prove that $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if $k = mn$ and m, n are relatively prime.
(b) Assume the classification of finitely generated abelian groups stated in class. Prove: If A is a finitely generated abelian group, it is isomorphic to a group of the form

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

where n_i divides n_{i+1} for all $1 \leq i \leq k-1$.

Groups

18. Your common mistakes

(a) Give an example of a group G, and an abelian subgroup $H \subset G$, such that H is not normal in G.
(b) Given an example of a group G, and a sequence of subgroups

$$G_1 \subset G_2 \subset G$$

such that $G_1 \triangleleft G_2$ and $G_2 \triangleleft G$, but G_1 is not normal in G.

19. Sylow's Theorems

Let n_p denote the number of Sylow p-subgroups of G.

(a) * Let $G = S_4$. Compute n_2.
(b) Let $G = S_4$. Compute n_3.
(c) Let $G = D_{2p}$, the dihedral group with $2p$ elements, where $p > 2$ is a prime. Compute n_2 and n_p.

20. Actions and orbit-stabilizer

(a) Show that $H \triangleleft G$ if and only if the normalizer of H is all of G.
(b) Let G be a finite group, and $H \subset G$ a subgroup. Show that the number of subgroups of G conjugate to H is equal to the size of G, divided by the order of the normalizer of H.
(c) Let $x \in G$ be an element, with $|G|$ finite. Show that the number of elements conjugate to x is equal to the size of G, divided by the number of elements that commute with x.

21. Prove Lagrange's Theorem

Prove Lagrange's Theorem.

22. Cayley's Theorem

(a) Show that every group acts on itself.
(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem.

23. Groups of order 8

Recall the quaternion ring, otherwise called the Hamiltonians. Consider the set

$$Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{R}^4$$

where

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

(a) Show that Q is a group of order 8.
(b) Show that Q is non-abelian.
(c) Write down all subgroups of Q.
(d) * Show that Q is not isomorphic to $D_{2\cdot 4} = D_8$, the dihedral group with 8 elements.

24. Some big theorems

(a) Let p be a prime number. If $n \in \mathbb{Z}$ is not divisible by p, prove that

$$n^{p-1} - 1$$

is divisible by p. This is called Fermat's Little Theorem. (Hint: If $\mathbb{Z}/p\mathbb{Z}$ is a field, what can you say about $\mathbb{Z}/p\mathbb{Z} - \{0\}$?)
(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem. (Hint: Every group acts on itself by left multiplication.)

Terms you'll need to know

(1) Group
(2) Finite group
(3) Isomorphism
(4) Subgroup
(5) Homomorphism
(6) Trivial homomorphism (i.e., one whose image is $\{1\}$)
(7) Order of an element g (size of $\langle g \rangle$—equivalently, smallest $n \geq 1$ for which $g^n = 1$. Orders can be infinite.)
(8) Order of a group (number of elements in the group—possibly infinite.)
(9) Abelian group
(10) p-Sylow subgroup
(11) Normal subgroup
(12) Quotient group
(13) Simple group
(14) Automorphisms of a set (i.e., a bijection from a set to itself)
(15) Automorphisms of a group (i.e., a group isomorphism from a group to itself)
(16) Group action
(17) Orbits
(18) Disjoint union
(19) Center of a group (the set of all x such that $gx = xg$ for all $g \in G$.)
(20) Direct product of groups
(21) Semidirect product
(22) Characteristic polynomial of a matrix with entries in a field F
(23) Ring
(24) Multiplicative identity of a ring
(25) Additive identity of a ring
(26) Ring homomorphism (remember that 1 must be sent to 1!)
(27) Left R-module (sometimes, simply called an R-module; especially if R is commutative)
(28) A homomorphism of left R-modules (a.k.a. R-linear map)
(29) Direct sum $M \oplus N$ of R-modules
(30) Ideals
(31) Ideal generated by a single element
(32) Quotient rings
(33) Field
(34) Vector space (i.e., a module over a field)
(35) Algebraically closed field
(36) Polynomial ring $F[t]$

(37) Irreducible polynomial
(38) Upper triangular matrix
(39) Cayley-Hamilton Theorem
(40) Relatively prime numbers (i.e., those such that $gcd = 1$.)

Some of the ideas you'll want to know (emphasis on "some")

(1) How to pass from semidirect products to split short exact sequences (Given $L \rtimes_\phi R$, there is the inclusion $L \to L \rtimes_\phi R$ given by $l \mapsto (l, 1_R)$ and $j : R \to L \rtimes_\phi R$ given by $j(r) = (1_L, r)$. Then the short exact sequence $L \to L \rtimes_\phi R \to R$ is split by j.)
(2) How to pass from split short exact sequences to semidirect products ($L \to H \to R, j : R \to H$ means $j(R)$ acts on L by conjugation, meaning one has a homomorphsim $\phi : R \cong j(R) \to \mathrm{Aut}(L)$, so a semidirect product $L \rtimes_\phi R$. You haven't lost information because the map $L \rtimes_\phi R \to H$ given by $(l, r) \mapsto l \cdot j(r)$ is an isomorphism, and $L \rtimes_\phi R$ has the obvious split short exact sequences $L \to L \rtimes_\phi R \to R, R \to L \rtimes_\phi R$. We are identifying L with its image in H.)
(3) Classify all abelian groups of finite order
(4) Classification theorem of finitely generated modules over a PID
(5) Using Sylow's Theorems to count Sylow subgroups
(6) Characteristic polynomials don't change under conjugation—so $\det(tI - A) = \det tI - BAB^{-1})$, regardless of the field in which the A takes entries.

Math 122 Fall 2014 Solutions to Practice Problems for Final

Practice Problems for matrices and Cayley-Hamilton

1. Basics in characteristic polynomials

(a) Let F be a field, and A a $k \times k$ matrix with entries in F. Show that A is not conjugate to an upper-triangular matrix unless its characteristic polynomial can be factored into (possibly non-distinct) linear polynomials in $F[t]$.

(b) Given an example of a matrix in a field F whose characteristic polynomial cannot be factored into linear polynomials.

(c) Prove that if A is a $k \times k$ matrix with entries in a field F, its characteristic polynomial $\Delta(t)$ is a degree k polynomial in $F[t]$, and that the degree $k-1$ coefficient of $\Delta(t)$ is $-\mathrm{tr}(A)$. (Here, $\mathrm{tr}(A)$ is the trace of A—the sum of its diagonal entries.)

(d) Prove that the constant term of $\Delta(t)$ is $(-1)^k \det A$.

(a) Suppose that A is conjugate to an upper-triangular matrix, so $T = BAB^{-1}$ where T is upper-triangular and B is invertible. Recall the characteristic polynomial of T and A are the same, because

$$\det(tI - T) = \det(tI - BAB^{-1}) = \det(B(tI - A)B^{-1}) = \det B \det B^{-1}(tI - A) = \det(tI - A).$$

On the other hand,

$$tI - T = \begin{bmatrix} t - T_{11} & -T_{12} & \dots & -T_{1k} \\ 0 & t - T_{22} & \dots & -T_{2k} \\ & & & \\ 0 & 0 & \dots & \vdots \\ 0 & 0 & \dots & t - T_{kk} \end{bmatrix}$$

is an upper-triangular matrix, so its determinant is given by multiplying its diagonal entries:

$$\det(tI - T) = (t - T_{11}) \dots (t - T_{kk})$$

so the characteristic polynomial of A factors into linear polynomials.

(b) Let us choose $\mathbb{R} = F$ to be our field. We know $\mathbb{R}$ has no square root of -1, so we reverse-engineer a matrix whose characteristic polynomial is $t^2 + 1 = 0$. For instance,

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

(c) For a field F, consider an injective ring homomorphism $F \hookrightarrow \overline{F}$ into an algebraically closed field $\overline{F}$. Any matrix $A \in M_{k \times k}(F)$ is conjugate to an upper-triangular matrix with entries in $\overline{F}$ (by the classification

of finitely generated modules over PIDs). And the characteristic polynomial of an upper-triangular matrix is

$$\det(tI - T) = (t - T_{11}) \dots (t - T_{kk})$$

which is clearly a degree k polynomial. Moreover, the characteristic polynomial of A is unchanged by conjugation, so we conclude that the characteristic polynomial of A is also degree k. (Note that each linear factor, $t - T_{ii}$, is a polynomial in $\overline{F}[t]$, but may not be a polynomial in $F[t]$.) To prove the statement about trace: Note that the degree $k-1$ portion of the above polynomial is given by

$$-T_{11} - \dots - T_{kk} = -tr(T).$$

But trace is also left unchanged by conjugation. Here is a two-step proof: First,

$$\mathrm{tr}(AB) = \sum_{i=1}^{k} (AB)_i i = \sum_{i=1}^{k}\sum_{j=1}^{k} A_{ij}B_{ji} = \sum_{i=1}^{k}\sum_{j=1}^{k} B_{ji}A_{ij} = \sum_{j=1}^{k}\sum_{i=1}^{k} B_{ji}A_{ij} = \sum_{j=1}^{k} (BA)_{jj} = \mathrm{tr}(BA).$$

Plugging in $B = D^{-1}C$ and $A = D$, we see that

$$\mathrm{tr} D^{-1}CD = \mathrm{tr} C$$

Since the trace of T is given by $-\mathrm{tr}(T)$, the trace of the original matrix is also given by negative its trace.

(d) Here are two proofs: Again, use that determinants are also unchanged by conjugation. So $\det(A) = \det(T)$ if T is an upper-triangular matrix conjugate to A. The constant term of $(t - T_{11}) \dots (t - T_{kk})$ is obviously $(-1)^k \det T$ (since it is the product of the diagonal entries of T) so the constant term of $\det(tI - A)$ is also $(-1)^k \det T = (-1)^k \det A$. For a second proof, recall that if $f : R \to S$ is a ring homomorphism, and if $F : M_{k\times k}(R) \to M_{k\times k}(S)$ is the induced map on matrices, then $f(\det A) = \det F(A)$ for every matrix A. Evaluating a polynomial at $t = 0$ is a ring homomorphism from $F[t] \to F$, so given the characteristic polynomial of $tI - A$, we have that

$$\det(0I - A) = \det(-A) = (-1)^k A.$$

On the other hand, evaluating any polynomial at $t = 0$ simply recovers the constant term of the polynomial.

2. Matrices are linear transformations

Let R be a commutative ring and $R^{\oplus k}$ the free module on k generators. Show there is a ring isomorphism

$$T : M_{k\times k}(R) \to \hom_R(R^{\oplus k}, R^{\oplus k})$$

given by sending a matrix A to the homomorphism T_A sending the ith standard basis element of $R^{\oplus k}$ to the element

$$\sum_{j=1}^{k} A_{ji} e_j.$$

If you are lazy and don't want to do every part of the proof, here is the most important part: prove that $T_{AB} = T_A \circ T_B$, so that matrix multiplication is sent to composition of functions.

Remark 2.1. (Recall that a homomorphism from $R^{\oplus k}$ to any module M is determined by the choice of k elements $x_1, \ldots, x_k$ in M, simply be declaring that $e_i \in R^{\oplus k}$ get sent to x_i.)

Remark 2.2. To be clear, the target of T is the set of all left R-module homomorphisms from $R^{\oplus k}$ to itself.

Remark 2.3. By the way, this ring isomorphism is the justification for saying that a linear map from a finite-dimensional vector space over F to itself is the same thing as a matrix—in this case, $R = F$, and every finite-dimensional vector space over F is isomorphic to $F^{\oplus k}$ for some k.

Let e_i denote the ith standard basis element of $R^{\oplus k}$—it is the element which has the multiplicative unit 1 in the ith coordinate, and 0 elsewhere. Let A be a matrix. By definition, T assigns to A the linear transformation taking e_i to the element

$$\sum_{j=1}^{k} A_{ji} e_j \in R^{\oplus k}.$$

This defines the R-linear map T_A completely, as a module homomorphism from a free module is determined by what it does to the standard basis elements. We show that T defines a ring homomorphism:

(1) *T sends the multiplicative identity to the multiplicative identity.* The identity of $M_{k\times k}$ is the identity matrix I, whose entries consist of 1 along the diagonal and 0 elsewhere. Then T_I sends e_i to $\sum A_{ji} e_j = e_i$, so T_I acts as the identity on the standard basis elements. For any other element $v = \sum a_j e_j$ then, $T_I(v) = T_I(\sum a_j e_j) = \sum a_j T_I(e_j) = \sum a_j e_j = v$. So T_I is indeed the identity homomorphism from $R^{\oplus k}$ to itself.

(2) $T(A+B) = T_A + T_B$. The matrix $A+B$ has (i,j)th entry given by $A_{ij} + B_{ij}$. Then $T_{A+B}(e_i) = \sum (A+B)_{ji} e_j = \sum (A_{ji} + B_{ji}) e_j = \sum A_{ji} e_j + \sum B_{ji} e_j = T_A(e_i) + T_B(e_i)$. It follows that for an arbitrary vector v, $T_{A+B}(v) = T_A(v) + T_B(v)$.

(3) $T_{AB} = T_A \circ T_B$. Note that the (j,i)th entry of the matrix AB is given by $(AB)_{ji} = \sum_l A_{jl} B_{li}$. Then $T_{AB}(e_i) = \sum_j (\sum_l A_{jl} B_{li}) e_j = \sum_l \sum_j A_{jl} B_{li} e_j = \sum_l T_A(B_{li} e_l) = T_A(\sum_l B_{li} e_l) = T_A(T_B(e_i))$. Since $T_{AB}(e_i) = T_A \circ T_B(e_i)$ for all standard basis elements e_i, it follows that $T_{AB}(v) = T_A \circ T_B(v)$ for all elements $v \in R^{\oplus k}$, so $T_{AB} = T_A \circ T_B$.

3. Some Cayley-Hamilton applications

Let $\mathbb{F}$ be a field of characteristic p. Let A be an upper-triangular $k \times k$ matrix with entries in $\mathbb{F}$.

(a) Assume A's diagonal entries are equal to 1. Show that for the values $(3,3)$, $(5,5)$, and $(4,2)$ of (k,p), A^k is equal to $(-1)^{k-1}I$.

(b) With the hypothesis as in part (a), prove that A is an element whose order must divide k or $2k$.

(a) The determinant of $tI - A$ is given by

$$\det \begin{bmatrix} t-1 & -A_{12} & \dots & -A_{1k} \\ 0 & t-1 & \dots & -A_{2k} \\ & & & \vdots \\ 0 & 0 & \dots & t-1 \end{bmatrix} = (t-1)^k.$$

By the binomial theorem, this means that the determinant of $tI - A$ is given by the polynomials

$$t^3 - 3t^2 + 3t - 1, \qquad t^4 - 4t^3 + 6t^2 - 4t + 1, \qquad t^5 - 5t^4 + 10t^3 - 10t^2 + 5t - 1$$

for $k = 3, 4, 5$ respectively. If F is a field of characteristic 3, the first polynomial is $t^3 - 1$, so by Cayley-Hamilton, $A^3 = I$. If F is a field of characteristic 2, the second polynomial is $t^4 + 1$, so by Cayley-Hamilton, $A^4 = -I$. In characteristic 5, the last polynomial is $t^5 - 1$, so by Cayley-Hamilton, $t^5 = I$.

(b) If $A^k = (-1)^{k-1}I$, if k is odd, clearly $A^k = I$, so the order of A as an element of $GL_k(F)$ must divide k. Likewise, if k is even, then $A^{2k} = (-I)^2 = I$, so the order of A must divide $2k$.

4. More Cayley-Hamilton

Let F be a field and A an $k \times k$ matrix with entries in F. When you want to compute $f(A)$ where $f(t)$ is some high-degree polynomial in t, note that by the division algorithm for polynomials, we can write

$$f(t) = q(t)\Delta(t) + r(t)$$

where $\Delta(t)$ is the characteristic polynomial of A. Then we have

$$f(A) = q(A)\Delta(A) + r(A) = r(A)$$

since $\Delta(A) = 0$ by the Cayley-Hamilton theorem. This reduces a potential costly calculation into two steps: A division of polynomials (to find r) and then a degree $k-1$ computation given by evaluating $r(A)$.

(a) If A is a 2×2 matrix which is not invertible in F, prove that A^2 is always a scalar multiple of A. Moreover, prove that A^2 is obtained from A by scaling via the trace of A.

(b) Let A be a 3×3 matrix which is not invertible, and which has trace zero. Compute A^{1000} in terms of A^2 and the degree 1 coefficient of $\Delta(t)$. Derive a general formula for A^N in terms of A^2 and the degree 2 coefficient of $\Delta(t)$.

(c) Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 5 & 2 & -1 \end{bmatrix}.$$

Compute A^{2014} using the methods above.

(d) What is A^{2014} if you consider A as a matrix with entries in $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$?

(a) If A is not invertible in a field F, then its determinant must be zero. (Recall a matrix is invertible in a ring if and only if its determinant is a unit int he ring.) Since the constant term of the characteristic polynomial of A is the determinant, Cayley-Hamilton tells us A must satisfy the equation

$$A^2 + aA = 0$$

where $t^2 + at$ is the characteristic polynomial of A. Hence $A^2 = -aA$, and A^2 is some scalar multiple of A.

(b) By before, the determinant of A is $(-1)^{k-1}$ times the constant term of the characteristic polynomial, while the trace is -1 times the degree $(k-1)$ term fo the characteristic polynomial. So if both of these is zero, the characteristic polynomial of A is of the form $t^3 - at$ for some number $a \in F$. So let us divide the polynomial t^{1000} by this polynomial and find the remainder. We find that

$$t^{1000} = (t^3 - at)q(t) + r(t)$$

where $q(t) = t^{997} + at^{995} + a^2t^{993} + a^3t^{991} + \ldots + a^{498}t$, or

$$q(t) = \sum a^i t^{1000-3-2i},$$

and $r(t) = a^{499}t^2$. Let us evaluate this polynomial on A:

$$A^{1000} = (A^3 - aA)q(A) + r(A).$$

Sine $A^3 - aA$ is the chracteristic polynomial of A, by Cayley-Hamilton, it evaluates to zero. Hence

$$A^{1000} = r(A) = a^{499}A^2$$

where a is the degree 1 coefficient of the characteristic polynomial. More generally, if we divide the polynomial t^N by the characteristic polynomial, we have that

$$q(t) = \sum a^i t^{N-3-2i}$$

so if i is the largest integer for which $N - 3 - 2i > 0$,

$$A^N = r(A) = a^{i+1}t^{N-3-2i+1}.$$

Note that $N - 3 - 2i + 1$ must be equal to 1 or to 2.

(c) Let us compute the characteristic polynomial of A:

$$\det(tI - A) = \det \begin{bmatrix} t-1 & -2 & -3 \\ -1 & t & 1 \\ -5 & -2 & t+1 \end{bmatrix}$$

which equals

$$(t-1)[t^2 + t + 2] + 2(-t - 1 + 5) - 3(2 + 5t) = t^3 - 16t.$$

Now, $2014 - 3 = 2011$, so the value of i from the previous problem is 1005. So by the above work, we know that A^{2014} must equal

$$A^{2014} = 16^{1006}A^2.$$

(d) If F has characteristic 2, $16x = 0$ for any $x \in F$, so the entries of the matrix $16^{1006}A^2$ are all zero. So $A^{2014} = 0$.

Rings and ideals

5. Basics of rings

(a) Give an example of a non-commutative ring with a zero divisor. (Make sure to identify the zero divisor.)
(b) Given an example of a commutative ring with a zero divisor.

(a) Consider the ring of 2 by 2 matrices with real entries. Then the elements

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

satisfy

$$AB = 0.$$

Hence both B and A are zero divisors in this ring. (Indeed, we can consider A and B as matrices with coefficients in any ring R with $1 \neq 0$, and these would be examples of zero divisors in the ring $M_{2\times 2}(R)$.) Note that although $AB = 0$, $BA = A \neq 0$.

(b) Consider the ring $\mathbb{Z}/6\mathbb{Z}$. Then $\overline{2} \cdot \overline{3} = \overline{6} = 0$. Or, if you consider the ring $\mathbb{R}[t]/(t^2)$, we have that $\bar{t} \cdot \bar{t} = \bar{t}^2 = 0$.

6. Prime ideals

Let R be a commutative ring. An ideal I is called *prime* if whenever $xy \in I$, we have that either $x \in I$ or $y \in I$.

(a) Let $f \in R$ be an irreducible element and R a PID. Show that the ideal generated by f is prime.

(b) Recall that a commutative ring is called a *domain* if it has no zero divisors. Show that if I is a prime ideal of R, then R/I is a domain.

(a) Let $xy \in (f)$. This means that $xy = af$ for some $a \in R$. Since R is a PID, every element allows for unique factorization by irreducibles. That means that $x = \prod q_i$ for some irreducibles q_i, possibly repeated, and $y = \prod p_i$. Then $xy = \prod q_i \prod p_i$ is a factorization of xy by primes. At the same time, since $a \in R$, a also has a prime factoriation $a = \prod r_i$ where each r_i is some irreducible element. Note that $af = f \prod r_i$ is a prime factorization for af, and hence for xy. By uniqueness of prime factorization, f—or a unit multiple of it—must show up in the product $\prod q_i \prod p_i$. This means $f = u'p_i$ or $u'q_i$ for some i and some unit u'. Without loss of generality assume $f = u'p_i$. Then f divides x, hence $x \in (f)$.

(b) By definition, $\overline{f} = 0 \in R/I$ if and only if $f \in I$. Well, for $\overline{x}, \overline{y} \in R/I$, we have that $xy \in I \implies x \in I$ or $y \in I$. Hence if $\overline{x} \cdot \overline{y} = 0$, we have that $\overline{x} = 0$ or $\overline{y} = 0$.

7. Prime ideals and maximal ideals

Let R be a commutative ring.

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

(a) Let $I \subset R$ be a maximal ideal. Let $xy \in I$. If x is not in I, let (I, x) be the smallest ideal containing I and x. (This is the image of the R-module homomorphism $I \oplus R \to R$ sending $(f, 1) \mapsto f + x$ for $f \in I$.) This must be equal to R since $I \subset (I, x) \subset R$ and I is maximal. Hence it contains $1 \in R$. This means

$$1 = f + gx$$

for some $f \in I, g \in R$. But then $y = fy + gxy$ by multiplying both sides by y on the right. So the righthand side is a sum of two elements in I. That is, $y \in I$.

(b) Suppose I is a prime ideal in a PID R. Then $I = (f)$ for some $f \in R$ since R is a PID. We assume $f \neq 0$ since we can assume $I \neq \{0\}$. If $xy \in I$, then either x or y is divisible by f by definition of prime ideal. Now, if we have an ideal $I \subset J \subset R$, then $J = (z)$ by definition of PID, and $I \subset J \implies f = az$ for some $a \in R$. By the previous discussion, either a or z is divisible by f. If z is, then $(z) \subset (f)$, so $J = I$. If a is, then $f = a'fz \implies 0 = f - a'fz = (1 - a'z)f$. If $I \neq \{0\}$, then since R is a domain, $a'z = 1$, so z is a unit, meaning $J = R$. Thus $I \subset J \subset R \implies J = I$ or $J = R$ whenever I is a prime ideal. That is, in a PID, every prime ideal I is maximal.

8. A ring that is not a PID

(a) Let F be a field, and let $R = F[x_1, x_2]$ be the ring of polynomials with two variables. Exhibit an ideal in R that is not principal.
(b) Show that $\mathbb{Z}[x]$—the ring of polynomials with $\mathbb{Z}$ coefficients—is not a principal ideal domain.

(a) Let $I = (x_1, x_2)$ be the ideal generated by the polynomial x_1, and by the polynomial x_2. So this is the set of all polynomials that have no constant terms. If there is some polynomial f such that $af = x_1$ for $a \in R$, we must have that f is constant, or is equal to some multiple of x_1. Likewise, if there is some polynomial f such that $bf = x_2$, we must have that f is constant, or is equal to some constant multiple of x_2. If a single polynomial f generates both x_1 and x_2, f must therefore be a constant polynomial (non-zero by assumption). But since f would then be a unit, $(f) = R$, so the only principal ideal containing (x_1, x_2) is R itself. That is, I cannot be a principal ideal.
(b) Let $R = \mathbb{Z}[x]$. Consider the ideal I generated by $2 \in \mathbb{Z}$ and by the polynomial $x \in \mathbb{Z}[x]$. This is the image of the homomorphism $R \oplus R \to R$ where $(a, b) \mapsto 2a + bx$. Let (f) be a principal ideal containing I—then there must exist $p \in R$ such that $pf = 2$, and $q \in R$ such that $qf = x$. That $pf = 2$ means f must equal ± 1 or ± 2. That $qf = x$ means that f must equal ± 1 or $\pm x$. This means $f = \pm 1$, so f is a unit in R, and we have that $(f) = R$. So the only principal ideal containing I is R itself, and I is not a principal ideal.

Modules

9. $\mathbb{Z}$-modules

(a) Show that a $\mathbb{Z}$-module is the same thing as an abelian group.
(b) Show that a map of $\mathbb{Z}$-modules (i.e., a $\mathbb{Z}$-linear homomorphism between $\mathbb{Z}$-modules) is the same thing as a homomorphism of abelian groups.

(a) Let M be an abelian group. To give M the structure of a $\mathbb{Z}$-module, we must exhibit a map

$$\mathbb{Z} \times M \to M$$

such that $(a+b)x = ax+bx$, $1x = x$ (where 1 is the multiplicative unit of $\mathbb{Z}$) and $(ab)x = a(bx)$ for all $a, b \in \mathbb{Z}, x \in M$. Well, every element of $\mathbb{Z}$ can be expressed as $a = 1 + \ldots + 1$, or as $a = -1 + \ldots + -1$ where the summation runs $|a|$ times. Hence

$$ax = (1+\ldots+1)x = x+\ldots+x \qquad (a \geq 0), \qquad ax = -(1+\ldots+-1)x = -x+\ldots+-x \qquad (a \leq 0)$$

so the map $\mathbb{Z} \times M \to M$ is completely determined by the abelian group structure of M. In other words, for any set M, the collection of abelian group structures on M is in bijection with the collection of $\mathbb{Z}$-module structure on M.

(b) Let M and N be $\mathbb{Z}$-modules. Note that the set $\mathcal{F}$ of $\mathbb{Z}$-module homomorphisms from M to N has a function to the set $\mathcal{H}$ of abelian group homomorphisms $M \to N$, since every R-module homomorphism is by definition an abelian group homomorphism (together with an additional property). We show that this function is a bijection. It is obviously an injection. It is also a surjection: A $\mathbb{Z}$-module homomorphism $f : M \to N$ is an abelian group homomorphism such that $f(ax) = af(x)$. Well, since any $a \in \mathbb{Z}$ can be expressed as a sum of 1 (as above), we have that

$$f(ax) = f(x + \ldots + x) = f(x) + \ldots + f(x) = af(x)$$

where the middle equality follows from the fact that f is a group homomorphism. So any abelian group homomorphism is automatically a $\mathbb{Z}$-module homomorphism.

10. $\mathbb{Z}[t]$-modules

Show that a $\mathbb{Z}[t]$-module structure on an abelian group M is the same thing as giving an abelian group homomorphism from M to itself.

Let $\mathcal{I}$ be the set of all ring homomorphisms from $\mathbb{Z}[t]$ to the set $\mathrm{End}(M)$ of endomorphisms of M to itself. By previous homework, we know this is in bijection with the set of all $\mathbb{Z}[t]$-module structures on M. So we will show that the set of ring homomorphisms from $\mathbb{Z}[t]$ to any target ring S is in bijection with elements of S. This shows that the set of module structures on M is in bijection with elements of $\mathrm{End}(M)$. Well, if $f : \mathbb{Z}[t] \to S$ is a ring homomorphism, we have an element $f(t) \in S$. On the other hand, since f is a ring homomorphism, and $f(1) = 1_S$, the value of $f(t)$ determines the value of f on every element of $\mathbb{Z}[t]$:

$$\begin{aligned} f(a_0 + a_1 t + \ldots a_k t^k) &= f(a_0) + f(a_1 t) + \ldots + f(a_k t^k) \\ &= f(1 + \ldots + 1) + f((1 + \ldots + 1) \cdot t) + \ldots + f((1 + \ldots + 1) \cdot t \cdot \ldots \cdot t) \\ &= (f(1) + \ldots + f(1)) + (f(t) + \ldots + f(t)) + (f(t)^k + \ldots + f(t)^k) \end{aligned}$$

where the summations happen $a_0, a_1, \ldots, a_k$ times, and if a_i is negative, we mean the summation $-1 + \ldots + -1$ with $|a_i|$ many terms. Thus, if $f(t) = f'(t)$, then $f = f'$, so this assignment is an injection. On the other hand, an arbitrary choice of element $s \in S$ determines a ring homomorphism f by assigning $f(t) = s$, and extending by the equation above. So the assignment $f \mapsto f(t)$ is a surjection as well.

11. Submodules

Let M be a left R-module. Recall that an *R-submodule* of M is a subgroup $N \subset M$ such that $rx \in N$ for all $r \in R, x \in N$.

(a) Show that the intersection of two submodules is a submodule.
(b) If R is a commutative ring and $R = M$, show that a submodule of M is the same thing as an ideal of R.

(a) The intersection of two subgroups is a subgroup. On the other hand, if $x \in N \cap N'$, then $rx \in N$ and $rx \in N'$ if N, N' are submodules. Hence $rx \in N \cap N'$.
(b) By definition, an ideal I of a commutative ring R is a subgroup of R for which $x \in I \implies rx \in I$ for all $r \in R$. Well, every ring R is a module over itself, with an R-module structure given by the function

$$R \times R \to R, \qquad (x, y) \mapsto xy$$

and by associativity and distributivity, this turns R into a left module over itself.

12. Not all modules are free

Give an example of a ring R and a left module M such that M is not isomorphic to a free R-module.

Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ for $|n| \geq 2$. Then $\mathbb{Z}/n\mathbb{Z}$ has $|n| \geq 2$ elements, while $R^{\oplus k}$ has either infinitely elements, or 1 element (if $k = 0$). Hence the two sets cannot be in bijection, let alone admit a module isomorphism between them.

Computations

13. Computations with matrices

Consider the matrices

$$\begin{bmatrix} 1 & 4 \\ 5 & 7 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}.$$

(a) Which of them are invertible as elements of $M_{2\times 2}(\mathbb{Z})$?
(b) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$?
(c) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$?

(a) Compute the determinants of each matrix. If they are equal to $\pm 1 \in \mathbb{Z}$, then the determinants are units in the ring $\mathbb{Z}$, hence the matrices are invertible in $\mathbb{Z}$.
(b) Now take the determinants of each matrix and reduce modulo 2. This is non-zero if and only if the matrix is invertible.
(c) Likewise, reduce the integer determinants modulo 7. This is non-zero if and only if the matrix is invertible.

14. Polynomial roots

Consider the polynomials

$$t^3 + 2t + 1, \qquad t^4 + 1, \qquad t^2 + 3.$$

(a) Which of these are irreducible elements of $\mathbb{Z}/2\mathbb{Z}[t]$?
(b) Which of these are irreducible elements of $\mathbb{Z}/3\mathbb{Z}[t]$?
(c) Which of these are irreducible elements of $\mathbb{Z}/5\mathbb{Z}[t]$?

For degree 3 and degree 2 polynomials, any factorization into non-units must have some factor of a linear polynomial, so irreducibility is equivalent to the absence of a root. So I'll leave those polynomials to you. But the fourth-degree polynomial is less trivial, since non-existence of a root doesn't guarantee irreducibility. For $p = 2, 5$, note that -1 admits a square root, since $1^2 = 1 = -1$ modulo 2, while $2^2 = 4 = -1$ modulo 5. So the polynomial $t^4 + 1 = (t^2 + 1)(t^2 + 1)$ modulo 2, and $t^4 + 1 = (t^2 - 2)(t^2 + 2)$ modulo 5. For $p = 3$, the process is more complicated—the only obvious strategy we have at our disposal in this class is to test by brute force whether the polynomial can be factored by degree 2 polynomials.

Classification of finitely generated PIDs

15. Statement

State the classification of finitely generated modules over a PID.

Let R be a principal ideal domain (PID). Suppose that M is a finitely generated R-module.[1] Then M is isomorphic to the module

$$R^{\oplus n_0} \oplus R/(p_1^{n_1}) \oplus \ldots \oplus R/(p_l^{n_l})$$

where $n_0 \geq 0$, $n_i \geq 1$, and $l \geq 0$ are integers, and each p_i is an irreducible element of R. If M is isomorphic to another module of the form

$$R^{\oplus m_0} \oplus R/(q_1^{m_1}) \oplus \ldots \oplus R/(q_k^{m_k})$$

where each q_i is an irreducible element, and $m_0 \geq 0, m_i \geq 1$, $k \geq 0$, then $k = l, m_0 = n_0$, and there is some re-ordering of indices so that q_i is a unit multiple of p_i and $n_i = m_i$ for all i. [2]

[1] This means that for some $k \geq 0$, M admits some homomorphism of R-modules, $R^{\oplus k} \to M$ which is a surjection.

[2] Of course, $R^{\oplus n_0}$ is given the usual R-module structure as a free R-module, while $R/(p_i^{n_i})$ is given the quotient module structure:

$$R \times R/(p_i^{n_i}) \to R/(p_i^{n_i}), \qquad (f, \overline{g}) \mapsto \overline{fg}.$$

16. Classifying abelian groups

(a) How does the theorem let us classify finitely generated abelian groups?
(b) Classify all abelian groups of order 12.
(c) Classify all abelian groups of order 16.

(a) Take $R = \mathbb{Z}$. This is a PID since every ideal of $\mathbb{Z}$ is equal to an ideal of the form $(n) = n\mathbb{Z}$ for $n \in \mathbb{Z}$. The irreducible elements of $\mathbb{Z}$ are those numbers $\pm p$ where p is a prime. Finally, any $\mathbb{Z}$-module is nothing more than an abelian group, so we can conclude that any finitely generated abelian group is isomorphic to an abelian group of the form

$$\mathbb{Z}^{\oplus n_0} \oplus \mathbb{Z}/(p_1^{n_1}) \oplus \ldots \oplus \mathbb{Z}/(p_l^{n_l}).$$

(b) The prime factorization of 12 is $3 \cdot 2 \cdot 2$. Because the size of the abelian group M must be 12, and the size of an abelian group as above is given by

$$p_1^{n_1} \cdot \ldots \cdot p_l^{n_l}$$

we see that the possible choices of p_i, n_i are as follows:

$$p_1 = 2, p_2 = 1, p_3 = 1, n_i = 1, \qquad p_1 = 2, p_3 = 1, n_1 = 2, n_2 = 1.$$

So M must be isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad \text{or} \qquad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

(c) Likewise, the possible choices for p_i and n_i are

$$p_1 = p_2 = p_3 = p_4 = 2, n_1 = n_2 = n_3 = n_4 = 1, \qquad p_1 = p_2 = p_3 = 2, n_1 = n_2 = 1, n_3 = 2,$$
$$p_1 = p_2 = 2, n_1 = n_2 = 2, \qquad p_1 = p_2 = 2, n_1 = 1, n_2 = 3, \qquad p_1 = 2, n_1 = 4.$$

So we have the possible groups

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \qquad \mathbb{Z}/16\mathbb{Z}.$$

17. Another way to phrase classification of abelian groups

(a) Let k, m, n be integers. Prove that $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if $k = mn$ and m, n are relatively prime.

(b) Assume the classification of finitely generated abelian groups stated in class. Prove: If A is a finitely generated abelian group, it is isomorphic to a group of the form

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

where n_i divides n_{i+1} for all $1 \leq i \leq k-1$.

(a) Let $(1,1) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since the order of this group is mn, we know that the order of $(1,1)$ must divide mn. On the other hand,

$$(1,1) + \ldots + (1,1) = (\overline{a}, \overline{a})$$

where the summation happens a times. For the first coordinate to equal zero, $\overline{a} = 0$ modulo m, and for the left coordinate to equal zero, we must have that a is a multiple of n. That is, a must be a multiple of both m and n. But since m and n are relatively prime, the smallest multiple of both m and n is mn itself. On the other hand, the order of any element must divide the order of the group containing it so we have that $a|mn$ and $mn \leq a$. This means $a = mn$, so $(1,1)$ generates the whole group. On the other hand, suppose that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$. Then we must have that $k = mn$ since isomorphic groups have the same order. If m, n are not relatively prime, then let $a = lcm(m,n) < mn$. Then any element $(x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ would have order dividing a[3]and in particular, order strictly less than mn. So $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ could not have any element of order mn, and in particular, cannot be cyclic.

[3]For $(x,y) + \ldots + (x,y) = (ax, ay)$. Since $a = bm$, $ax = b(mx) = 0 \in \mathbb{Z}/m\mathbb{Z}$. Likewise, since $a = nc, ay = 0 \in \mathbb{Z}/n\mathbb{Z}$. So (1,1) must have order dividing a.

Groups

18. Your common mistakes

(a) Give an example of a group G, and an abelian subgroup $H \subset G$, such that H is not normal in G.

(b) Given an example of a group G, and a sequence of subgroups

$$G_1 \subset G_2 \subset G$$

such that $G_1 \triangleleft G_2$ and $G_2 \triangleleft G$, but G_1 is not normal in G.

(a) Let $H \subset S_3$ be the subgroup generated by the 2-cycle (12). This is not normal, since (12) is conjugate to (13) but $(13) \notin H$. On the other hand, it is clearly abelian, since it's cyclic.

(b) Let $G = S_4$ and $G_2 = V$ be the group of order 4 in S_4 isomorphic to the Klein 4-group. V has elements

$$1, (12)(34), (13)(24), (23)(14).$$

Note that since V is abelian, any subgroup of it is normal in V—in particular, let G_1 be the subgroup generated by (12)(34). Then $G_1 \triangleleft G_2$. And $G_2 \triangleleft G$ since every element of S_4 with cycle shape given by two disjoint 2-cycles is in V, while every element of V is of this cycle shape. We know that the group generated by (12)(34) is not normal in S_4 itself—for instance, (12)(34) is conjugate to (13)(24), but the latter is not in the subgroup generated by the former.

19. Sylow's Theorems

Let n_p denote the number of Sylow p-subgroups of G.

(a) * Let $G = S_4$. Compute n_2.
(b) Let $G = S_4$. Compute n_3.
(c) Let $G = D_{2p}$, the dihedral group with $2p$ elements, where $p > 2$ is a prime. Compute n_2 and n_p.

(a) Since $|G| = 24 = 8 \cdot 3$, the Sylow theorems tell us that n_2 divides 3, and is equal to 1 modulo 2. Thus n_2 is equal to 3 or to 1. You can exhibit a subgroup of order 8, and show it is not a normal subgroup. Thus n_2 must equal 3.
(b) n_3 must divide 8, and be equal to 1 modulo 3. The only such numbers are 1 or 4. Well, there is an obvious subgroup of order 3 given by the group generated by (123). This group cannot be normal because it does not contain all elements with the same cycle shape—for instance, it does not contain (124). Hence n_3 must be 4. (Recall that, by the Sylow theorems, $n_p = 1$ if and only if there is only one Sylow p-subgroup.)
(c) n_p has to equal 1 because it must divide 2, and equal 1 modulo p. To compute n_2, note that n_2 must equal 1 modulo 2, while it must also divide p. So we show that $n_2 \neq 1$. Note that the element $g \in D_{2p}$ given by reflection is an element of order 2, so it generates a group of order 2. Note that if you conjugate g by a rotation of $2\pi/p$, you do not get back g. Hence $n_2 \neq 1$.

20. Actions and orbit-stabilizer

(a) Show that $H \triangleleft G$ if and only if the normalizer of H is all of G.
(b) Let G be a finite group, and $H \subset G$ a subgroup. Show that the number of subgroups of G conjugate to H is equal to the size of G, divided by the order of the normalizer of H.
(c) Let $x \in G$ be an element, with $|G|$ finite. Show that the number of elements conjugate to x is equal to the size of G, divided by the number of elements that commute with x.

(a) Definition of normalizer.
(b) Orbit-stabilizer theorem; G acts by conjugation on the set of all subgroups of G. The stabilizer of a subgroup is the normalizer, and the orbit of H is the set of all subgroups conjugate to H.
(c) G acts on itself by conjugation. The elements that fix x are those that commute with x. The orbit of x is the set of all elements conjugate to x.

21. Prove Lagrange's Theorem

Prove Lagrange's Theorem.

Let $H \subset G$ be a subgroup of a finite group G. Lagrange's Theorem says that $|H|$ must divide $|G|$. Note that H acts on G via multiplication:

$$H \times G \to G, \qquad (h, g) \mapsto hg.$$

Then G is a disjoint union of the orbits of the H-action:

$$G = \coprod_{orbits} \mathcal{O}$$

Claim: For each orbit, $|\mathcal{O}| = |H|$. If we have this claim, we see that

$$|G| = |H| + \ldots + |H|$$

so $|H|$ divides $|G|$. To prove this claim, note that the orbit of $1_G \in G$ is

$$\{h1_G \in G \text{ s.t. } h \in H\} = \{h \in G \text{ s.t. } h \in H\} = H$$

so the orbit of 1_G *is the set* H, meaning $|\mathcal{O}_{1_G}| = |H|$. On the other hand, if $\mathcal{O}_g$ is another orbit, we have a bijection $\mathcal{O}_1 \to \mathcal{O}_g$ by sending

$$x \mapsto xg \in \mathcal{O}_g, \qquad x \in \mathcal{O}_{1_G}.$$

This is a bijection because it has an inverse given by sending $hg \in \mathcal{O}_g$ to $hgg^{-1} \in \mathcal{O}_{1_G}$. Hence every orbit is in bijection with $\mathcal{O}_{1_G}$, meaning $|\mathcal{O}| = |H|$ for every orbit.

22. Cayley's Theorem

(a) Show that every group acts on itself.
(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem.

(a) There are two equivalent ways to exhibit a group action of G on a set X. By exhibiting a group homomorphism

$$\phi : G \to \mathrm{Aut}_{Set}(X)$$

or a function

$$G \times X \to X, \qquad (g, x) \mapsto gx$$

satisfying
(a) $1_G x = x$ for all $x \in X$,
(b) $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$.
A group G acts on itself by the function

$$G \times G \to G, \qquad (g, x) \mapsto gx$$

where gx is the group multiplication. (a) follows from the definition of identity, and (b) follows from associativity of G's multiplication.

(b) Since we have a group action, we have a group homomorphism $\phi : G \to \mathrm{Aut}_{Set}(X)$. If we show this is an injection, by the first isomorphism theorem, we have the group isomorphisms

$$G \cong G/\{1_G\} \cong \mathrm{image}(\phi) \subset \mathrm{Aut}_{Set}(X) \cong S_{|X|}.$$

This last group is the symmetric group on $|X|$ elements. To show ϕ is an injection, we must show that it has trivial kernel—that is, that $\phi_g = \mathrm{id}$ implies that $g = 1_G$. But this follows from the uniqueness of the identity element of a group.

23. Groups of order 8

Recall the quaternion ring, otherwise called the Hamiltonians. Consider the set

$$Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{R}^4$$

where

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

(a) Show that Q is a group of order 8.
(b) Show that Q is non-abelian.
(c) Write down all subgroups of Q.
(d) * Show that Q is not isomorphic to $D_{2\cdot 4} = D_8$, the dihedral group with 8 elements.

(a) Claim: Let R be a ring, and let $R^\times$ be the subset of all elements in R with a multiplicative inverse. (I.e., the set of units of R.) Then $R^\times$ is a group. Proof of claim: Since 1_R is a unit, with inverse itself, $R^\times$ has an identity by definition of 1_R. Multiplication is associative since multiplication in R is associative, and every element admits an inverse by definition of units for a ring. Now that the claim is proven, denote the quaternions by $\mathbb{H}$. Recall that the quaternions are a ring, and that every non-zero element of the ring admits a multiplicative inverse. (This was a homework problem.) Then it follows that $\mathbb{H} - \{0\}$ is a group (non-abelian, since $\mathbb{H}$'s multiplication is not commutative), with identity given by the multiplicative identity $(1,0,0,0)$ of $\mathbb{H}$. We must show that $Q \subset \mathbb{H} - \{0\}$ is a subgroup. In any ring, we have that $(-a)\cdot b = -(a\cdot b) = a\cdot(-b)$, so to show closure, it suffices to show that

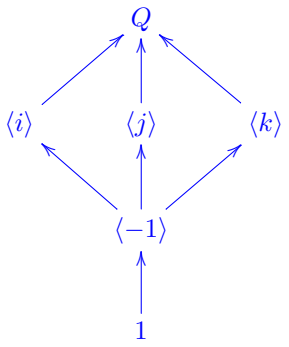
$$i \cdot j = k, \qquad i \cdot k = -j, \qquad j \cdot k = i$$

which you can check. Moreover, can see that for any $g \in Q$, $g\cdot(-g) = 1$, so every element has an inverse. Since $Q \subset \mathbb{H} - \{0\}$ is a subgroup, it is in particular a group. To check it has order 8, we simply count the elements—there are 8 of them.
(b) $ij = k$ while $ji = -k$.
(c) Tedious, but we can do this systematically as follows.
  (a) We have the subgroups generated by each element. So for instance,

$$\langle i \rangle = \{1, i, -1, -i\}$$

  is a subgroup of order 4, as are $\langle j \rangle$ and $\langle k \rangle$. These subgroups contain a unique subgroup of order 2, the one generated by -1. Note that $\langle -j \rangle = \langle j \rangle$.

(b) Now suppose that a subgroup contains both i and j. Then it contains $-1 = i^2, -i = i^3$, $k = ij$, and $-k = ji$. That is, the whole group. So we have that the subgroups of Q are given by



where the arrows indicate inclusions. Note that each of $\langle i \rangle, \langle j \rangle, \langle k \rangle$ are each subgroups of order 4, hence subgroups of index 2, hence normal.

(c) As a side note, observe that $\langle -1 \rangle = \{1, -1\}$ is the center of this group. As a result, $\langle -1 \rangle$ is normal in Q. It is the unique subgroup of order 2 in Q.

(d)

24. Some big theorems

(a) Let p be a prime number. If $n \in \mathbb{Z}$ is not divisible by p, prove that

$$n^{p-1} - 1$$

is divisible by p. This is called Fermat's Little Theorem. (Hint: If $\mathbb{Z}/p\mathbb{Z}$ is a field, what can you say about $\mathbb{Z}/p\mathbb{Z} - \{0\}$?)

(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem. (Hint: Every group acts on itself by left multiplication.)

(a) If p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. So $\mathbb{Z}/p\mathbb{Z} - \{0\}$ is a group. Let $\overline{n}$ be an element. Since $\mathbb{Z}/p\mathbb{Z} - \{0\}$ has order $p-1$, the order of $\overline{n}$ must divide $p-1$. Which is to say,

$$\overline{n}^{p-1} = \overline{1}$$

where $\overline{1}$ is the multiplicative unit of $\mathbb{Z}?p\mathbb{Z}$. So we have that for any $\overline{n} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$,

$$\overline{n}^{p-1} - \overline{1} = \overline{0} \in \mathbb{Z}/[\mathbb{Z}$$

So for any number n not divisible by p,

$$n^{p-1} - 1$$

equals zero modulo p—i.e., is divisible by p.

(b) We did this in a previous problem on this practice set.