Algebra Problem Sheets

Prof. Hiro Lee Tanaka

Contents

Problem Sheet 1

Getting a Feel for Groups

1.1 Pre-requisites

I assume you are familiar with basic notions of sets, injections, bijections, and proof. Other than that, the only facts you need are the following:

Definition 1.1 (What's a group?)**.** A group is a pair (G, m) where G is a set, and m is a map

$$m : G \times G \to G.$$

We will usually write[1]

$$m(g, h) := g \cdot h := gh.$$

The pair (G, m) must satisfy the following:

- (Identity) There exists an element $1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$.
- (Inverses) For every element $g \in G$, there exists an element (possibly different, possibly the same) g^{-1} such that $gg^{-1} = g^{-1}g = 1$, and
- (Associativity) $g(hk) = (gh)k$ for all $g, h, k \in G$.

The map m is called the group multiplication, the multiplication, or the group operation, of the group.

Remark. Be warned that $gh \neq hg$ in general. Note that we are already writing gh instead of $g \cdot h$, or of $m(g, h)$.

Remark. We will often write a group simply as G, and not (G, m), although m is necessarily part of the data. The notation G simply means that the group operation should be understood: For instance, $\mathbb{Z}$ is usually understood to mean the set of integers together with usual addition of integers as the group operation.

Remark. The existence of inverses allows us to use the cancellation law. That is, if a, b, c are elements of a group G, we have the implication

$$ab = ac \quad \Rightarrow \quad b = c.$$

This is because we can multiply both sides of the equation by a^{-1} and conclude $a^{-1}(ab) = (a^{-1}a)b = 1b = b$. Notice that we are using every property of a group——the identity, inverses, and associativity——in proving the cancellation law.

Definition 1.2 (Group Homomorphisms and Isomorphisms)**.** Let G and H be groups. A group homomorphism is a map of sets

$$\phi : G \to H$$

such that

$$\phi(gg') = \phi(g)\phi(g').$$

(i.e. ϕ represents multiplication.) An isomorphism of groups is a group homomorphism $\phi : G \to H$ which is also a bijection of sets.

Definition 1.3 (Subgroups)**.** Let G be a group. A subset $H \subset G$ is called a subgroup if

- H contains the identity of G,
- If $h \in H$, then $h^{-1} \in G$ is also in H, and
- If h and h' are in H, then so are hh' and $h'h$.

[1] Depending on context, we may sometimes write $g \cdot h$, while we may other times write gh for brevity. This is the same convention as in multiplying variables in standard high school algebra.

Goals: The goal of these problems is to start becoming familiar with the kinds of manipulations we'll wnat to do computations with groups.

1.2 Some Basics

Exercise 1.1.

(1) Show that the empty set does not admit a group structure.

(2) Show that the identity element of a group G is unique. (That is, if two elements 1 and $1'$ satisfy the defining property of the identity element, then $1 = 1'$.)

(3) Given an element $g \in G$, show that g^{-1} is unique. (That is, given elements h, h' satisfying the defining property of g^{-1}, show that $h = h'$.)

(4) Let G and H be two groups such that each group contains only one element. Show that G and H are isomorphic as groups. (That is, there is a unique group of cardinality 1.)

(5) Let G and H be two groups such that each group contains only two elements. Show that G and H are isomorphic as groups.

(6) If you have the free time, let G and H be two groups such that each group contains only three elements. Show that G and H are isomorpohic as groups. (This will become much easier to once we have Lagrange's Theorem.)

(7) Let $\phi : G \to H$ be a group isomorphism between two groups. Since ϕ is a bijection, there is a unique inverse map of sets $\psi : H \to G$. Show that ψ must be a group homomorphism.

(8) Show $g = g^2$ in a group G if and only if $g = 1$.

(9) If $\phi : G \to H$ is a group homomorphism, show that ϕ sends the identity of G to the identity of H.

(10) If $\phi : G \to H$ is a group homomorphism, show that $\phi(g^{-1}) = \phi(g)^{-1}$.

1.3 Orders of Group Elements

Exercise 1.2.

(1) Show that the non-zero complex numbers, written $\mathbb{C}^\times$, form a group under multiplication.

(2) For any element $g \in G$, we will always write the expression $g \cdot g \cdot \cdots \cdot g$ (with n appearances of g) as g^n. By convention, g^0 is the identity of a group. Show that for all $n \geqslant 0$ is the identity of a group. Show that for all $n \geqslant 0$, $\mathbb{C}^\times$ contains an element z for which $z^n = 1$.

(3) Given an element $g \in G$ of a group, the smallest, non-zero number n for which $g^n = 1$ is called the order of g. If g^n never equals 1, we say g is an element of infinite order. Show that $\mathbb{Z}$ only has elements of order 1 or infinity.

1.4 The Set of Automorphisms is a Group

We mentioned in class that groups are a useful language for describing symmetries of an object. What do we mean by a symmetry? A symmetry is an invertible operation from a mathematical object to itself, preseving some structure. Here we explore examples of this idea.

(1) Fix a set S. Let $\mathrm{Aut}(S)$ be the set of all bijections $S \to S$. Note there is a map $\mathrm{Aut}(S) \times \mathrm{Aut}(S) \to \mathrm{Aut}(S)$ given by composing bijections. Show that this gives a group structure on $\mathrm{Aut}(S)$. (Using the above philosophy, the mathematical object is a set S, and we view it as having no structure save the fact that S is a set.)

(2) Now fix a group G. Let $\mathrm{Aut}_{\mathrm{Group}}(G)$ be the set of all group isomorphisms from G to itself. Show that $\mathrm{Aut}_{\mathrm{Group}}(G)$ is itself a group. (Using the above philosophy, the mathematical object is G, and the structure we're preserving is its group structure——i.e., the identity and multiplication.)

(3) If you know what a topological space is, let X be a topological space, and $\mathrm{Aut}(X)$ the set of homeomorphisms from X to itself. Show that $\mathrm{Aut}(X)$ is a group.

(4) Fix $n \geqslant 1$. Show that $GL_n(\mathbb{C})$——the set of $n \times n$ complex, invertible matrices——form a group. Show the same is true for $GL_n(\mathbb{R})$. (Using the philosophy above, this is the set of all operations on an n-dimensional vector space that preserve the structure of linearity.)

(5) Fix $n \geqslant 1$. Show that $SL_n(\mathbb{C})$——the set of $n \times n$ complex matrices with determinant 1——form a group. Likewise for $SL_n(\mathbb{R})$. (Using the philosophy above, this is the set of all operations on an n-dimensional vector space that preserve the structure of linearity and oriented volume.)

(6) For any $n \geqslant 1$, show that $O(n)$——the set of $n \times n$ real orthogonal matrices——form a group. (Using the philosophy above, this is the set of all operations on an n-dimensional vector space that preserves the structure of linearity and inner product.)

1.5 Extras

Exercise 1.3.

(1) Let H and K be subgroups of G. Show their intersection is a subgroup.

(2) Given a group $G = (G, m)$, define the opposite group $G^{\text{op}} = (G, w)$ by the operation

$$w(g, h) := m(h, g).$$

That is, G^{op} as a set is the same set as G, but its multiplication happens in the opposite order. Show that G^{op} is a group.

(3) Show that the map $G \to G^{\text{op}}$ given by $g \mapsto g^{-1}$ is a group isomorphism.

(4) Let $\phi : G \to H$ be a group homomorphism. The kernel of ϕ, written $\ker \phi$, is the set of all g for which $\phi(g) = 1$. Show that the kernel of any group homomorphism is a subgroup of G.

(5) The image of ϕ is the set of all $h \in H$ such that $h = \phi(g)$ for some $g \in G$. Show that for any group homomorphism $\phi : G \to H$, the image of ϕ is a subgroup of H.

1.6 Linear Maps of Integers

Exercise 1.4. By the above exercise, the set $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$ is a group. (In fact, an abelian group.) Consider a 2×2 integer matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which defines a map $\mathbb{Z}^2 \to \mathbb{Z}^2$ in the usual way that matrices do. Specifically, given an element $(x, y) \in \mathbb{Z}^2$, the map sends

$$(x, y) \mapsto (ax + cy, bx + dy).$$

(1) Show that the above map is always a group homomorphism from $\mathbb{Z}^2$ to $\mathbb{Z}^2$.

(2) Determine when A is an injective group homomorphism, using the determinant of A.

(3) Determine when A is a group isomorphism, using the determinant of A.

1.7 Some Fun Linear Algebra

Exercise 1.5. Let n be an odd, non-zero integer. Show that every element of $O(n)$ has 1 as an eigenvalue. (Hint: What happens when you apply A^{T} to $A - I$?)

Problem Sheet 2

The Nature of Group Homomorphisms

2.1 Group Homomorphisms versus Maps of Sets

Exercise 2.1. Let $\phi_3 : \mathbb{Z} \to \mathbb{Z}$ be the map $\phi_3(n) = 3n$. So for instance, $\phi_3(2) = 6$. We think of the integers as a group under addition.

(1) Show that ϕ_3 is a group homomorphism.

(2) Show that there exists a map of sets $\psi : \mathbb{Z} \to \mathbb{Z}$ such that $\psi \circ \phi_3 = \mathrm{id}_{\mathbb{Z}}$.

(3) Show that no choice of such a ψ can be a group homomorphism.

(4) For any integer k, define a map of sets $\phi_k : \mathbb{Z} \to \mathbb{Z}$ by $\phi_k(n) = kn$. Show this defines a group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$. Determine all k for which this map is an isomorphism.

2.2 The Sign Representation

Exercise 2.2.

(1) Let S_n be the symmetric group on n elements. (Automorphisms of a set of n elements.) For every element $\sigma \in S_n$, let $\phi(\sigma)$ be the $n \times n$ matrix which sends the standard basis vector $e_i \in \mathbb{R}^n$ to the vector $e_{\sigma(i)}$. Show that the assignment $\phi : S_n \to GL_n(\mathbb{R})$ is a group homomorphism.

(2) List every element $\sigma \in S_3$ and write out the matrix $\phi(\sigma)$ for each of them.

(3) Show that the determinant defines a group homomorphism $\det : GL_n \to \mathbb{R}^\times$, which sends $A \mapsto \det A$. (You may use properties of determinants you learned form linear algebra class.) What is the special name we usually give to the kernel of this map?

(4) Consider the composite group homomorphism $S_n \to GL_n \to \mathbb{R}^\times$. We call this the sign representation of S_n. What is its image? (It is a subgroup of $\mathbb{R}^\times$.)

2.3 Centers

Exercise 2.3.

(1) For any group G, the center of G is the set of those g such that g commutes with all elements of G. That is, $gh = hg$ for all h. Show that the center of G is a normal subgroup of G.

(2) What is the center of $GL_n(\mathbb{R})$ for $n \geqslant 1$?

2.4 Using Divisibility

Exercise 2.4.

(1) Let G be a group of order p for some prime p. Let x be a non-indentity element of G. Show that x must have order p.

(2) Let G be a group of order p^n for some prime p and $n \geqslant 1$. Show that G must contain an element of order p.

(3) Let G be a group (possibly infinite). Let H and H' be finite subgroups. Show that if $\gcd(|H|, |H'|) = 1$, then $H \cap H' = \{1\}$.

2.5 Using Divisibility Again

Exercise 2.5.

(1) Let G be a finite abelian group. Show that the map $x \mapsto x^n$, for any integer $n \geqslant 0$, is a group homomorphism.

(2) Suppose further that $\gcd(|G|, n) = 1$. Show that the map $x \mapsto x^n$ is a group automorphism of G.

2.6 Free Groups

Exercise 2.6. What does a group with a set of generators, but with no relations look like? If the set of generators is S, this group is called the free group with generating set S. You will prove its existence, and its universal property, in this exercise.

Definition 2.1. Let $S = \{a, b, c, \ldots\}$ be a set. Though I have written a, b, c as though the elements may be enumerable (i.e. countable), S need not be countable. For $n \geqslant 0$, a word of length n in S is defined to be a map of sets $\{1, \ldots, n\} \to S$. The empty word is the map from the empty set to S, and is the unique word of length 0.

So a word of length n is simply an ordered string of n elements of S, possibly with repetitions.

Example 2.1. If $S = \{a, b, c\}$, then here are the words of lengths 0 to 2:

$$\varnothing \qquad \text{(the empty word)}$$

$$a, \qquad b, \qquad c$$

$$aa, \quad bb, \quad cc, \quad ab, \quad ba, \quad bc, \quad cb, \quad ca, \quad ac.$$

Here are some examples of words of length 5:

$$aaaba, \quad ababa, \quad acccb.$$

Given a set S, let $\overline{S}$ be the set given by adjoining a new element for every $s \in S$. we will write this new element as "s^{-1}" and call it the inverse of s. So for example, if $S = \{a, b, c, \ldots\}$, then

$$\overline{S} = \{a, a^{-1}, b, b^{-1}, c, c^{-1}, \ldots\}.$$

Definition 2.2. A word in $\overline{S}$ is called reduced if a letter in the word never appears next to its inverse.

Remark. As an example, here are some unreduced words, with unreduced bits underlined.

$$abba\underline{aa^{-1}}bcb\underline{cc^{-1}}b, \quad \underline{aa^{-1}}, \quad a\underline{b^{-1}b}b^{-1}c, \quad ab^{-1}\underline{bb^{-1}}c.$$

Given an unreduced word, we can make it reduced by simply removing two adjacent letters when one is the inverse of the other. For example, here are the reductions of the above words:

$$abbabcbb, \quad \varnothing, \quad ab^{-1}c, \quad ab^{-1}c.$$

Note that to fully reduce a word, one may require a few steps:

$$ab^{-1}\underline{cc^{-1}}ba^{-1} \to ab^{-1}ba^{-1} \to aa^{-1} \to \varnothing.$$

Regardless, since every word is by definition of finite length, this reduction process terminates. Given any word in $\overline{S}$, there is a unique reduction of that word, in which no letter appears next to its inverse.

Given two words w_1 and w_2, we may simply concatenate them (i.e., put them side by side) to create a new word. For instance, if

$$w_1 = abc, \quad w_2 = c^{-1}baa$$

then we have

$$w_1w_2 = abcc^{-1}baa, \quad w_2w_1 = c^{-1}baaabc.$$

(I've been told this is a common way to create new words in German.) Note that even if two words are reduced, their concatenation may not be. Also note that w_1w_2 need not equal w_2w_1.

Definition 2.3. Let S be a set. The free group on S is the set of reduced words of length $n \geqslant 0$ in $\overline{S}$. The group multiplication is given by concatenating two words, then reducing the concatenation.

(1) Show that any word in $\overline{S}$ admits a unique reduction.

(2) Show that the above operation is associative.

(3) Show that the free group is in fact a group.

(4) Let G be a group, and let $j : S \to G$ be a map of sets. Show that this extends to a group homomorphism $F(S) \to G$.

(5) Show there is a bijection of sets

$$\{\text{Group homomorphisms } F(S) \to G\} \cong \{\text{Set maps } S \to G\}.$$

Problem Sheet 3

Subgroups and Basic Group Constructions

3.1 Cosets of S_3 with respect to S_2

Exercise 3.1. Let S_3 be the symmetric group on 3 elements. Recall that this is the set of all bijections from $\underline{3}$ to itself, where $\underline{3} = \{1, 2, 3\}$. Let $H \subset S_3$ be the set of all bijections $\tau : \underline{3} \to \underline{3}$ such that $\tau(3) = 3$——i.e., the subset of all bijections that fix 3.

(1) Show H is a subgroup of S_3.

(2) So H acts on $G = S_3$. How many elements are there in the orbit space?

(3) Finally, write out each orbit explicitly. This means you must write out which elements of S_3 are in each orbit.

(4) For any $n \geqslant 1$, let $H \subset S_n$ be the subgroup of all elements that fix n. Exhibit an isomorphism from H to S_{n-1}.

(5) How many orbits are there of the action of H on S_n?

3.2 Cyclic Groups

Exercise 3.2. A group G is called cyclic if there exists $g \in G$ for which $\langle g \rangle = G$.

(1) Show that if two cyclic groups have the same order (finite or otherwise) then they must be isomorphic.

(2) Show that S_2 is cyclic.

(3) Show that $\mathbb{Z}$ is cyclic.

(4) Use Lagrange's theorem to show that any group of prime order must be cyclic. [Hint: Last homework.]

(5) Prove that for any integer $n \geqslant 1$, there exists a cyclic group of order n. For instance, as a subgroup of S_n, or of $GL_2(\mathbb{R})$, or of $\mathbb{C}^\times$.

3.3 Abelian Groups

Exercise 3.3. A group G is called abelian if for all $g_1, g_2 \in G$, we have $g_1 g_2 = g_2 g_1$.

(1) Show that S_n is not abelian for any $n \geqslant 3$.

(2) Show that any cyclic group is abelian. Conclude that S_n is not cyclic for any $n \geqslant 3$.

(3) Show that the center of an abelian group is the whole group.

3.4 Product Groups

Exercise 3.4. Let G and H be groups. Define a map

$$m : (G \times H) \times (G \times H) \to G \times H,$$
$$m((g,h),(g',h')) = (gg',hh').$$

Note that throughout this problem, 1 may refer to either the group unit of G, or the group unit of H.

(1) Show that m defines a group structure on $G \times H$.

(2) Show that $(g,1) \cdot (1,h) = (1,h) \cdot (g,1)$.

(3) Recall that a group A is called abelian if for all a, $a' \in A$, we have $aa' = a'a$. Show that if G and H are abelian, then $G \times H$ is abelian (with the above group structure).

(4) Show that $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ is a subgroup of $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

(5) Show that the maps

$$G \to G \times H,$$
$$g \mapsto (g,1)$$

and

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

are group homormophisms.

Problem Sheet 4

Conjugation in Group Theory

4.1 Subgroups of $\mathbb{Z}$

Exercise 4.1. In this problem, you will show that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geqslant 0$.

Let $H \subset \mathbb{Z}$ be a subgroup which contains some non-zero element. Let $n \in H$ be the least, positive integer inside H. Show that $H = n\mathbb{Z}$. [Hint: Remainders.]

4.2 Conjugation Actions

Exercise 4.2. The conjugation action of a group on itself is by far the most important group action in representation theory. A full understanding of the conjugation action can be illusive, and in many contexts, proves quite essential for research.

(1) Fix an element $g \in G$. Define a map $C_g : G \to G$ by $h \mapsto ghg^{-1}$. Show that C_g is a group isomorphism.

(2) Show that $C_g \circ C_{g'} = C_{gg'}$. In other words, the assignment $g \mapsto C_g$ defines a group homomorphism $G \to \mathrm{Aut}_{\mathrm{Group}}(G)$. So this defines another group action of G on itself. It is quite different from the action we have considered earlier, where all we had was a group homomorphism $G \to \mathrm{Aut}_{\mathrm{Set}}(G)$. This new map, $G \to \mathrm{Aut}_{\mathrm{Group}}(G)$, is called the conjugation action of G on itself.

(3) If G is abelian, show that C_g is trivial for all $g \in G$.

4.3 Group Isomorphisms in General

Exercise 4.3. Since C_g is a group isomorphism from G to itself, it tells us a lot about the subgroups and elements of G. This is because of some general properties of group isomorphisms, which we now explore. Let $\phi : G \to H$ be a group isomorphism. If $K \subset G$ is a subset, we define

$$\phi(K) = \{h \in H \text{ such that } h = \phi(g) \text{ for some } g \in K\}.$$

(1) Show that isomorphisms preserve orders of elements. That is, show that if g is an element of order n, then $\phi(g)$ is.

(2) Show that if $K \subset G$ is a subgroup, it is isomorphic to $\phi(K)$.

(3) Show that isomorphisms preserve normal subgroups. That is, show that if $K \subset G$ is a normal subgroup, then $\phi(K) \subset H$ is normal.

(4) Let K be a normal subgroup G. Show that there is a group isomorphism $G/K \cong H/\phi(K)$.

Throughout the following exercises, if you have time, think about what the above results imply about elements and subgroups of G that are conjugate.

4.4 Conjugacy Classes of Elements

Exercise 4.4.

(1) Two elements $g, g' \in G$ are called conjugate if there exists some $h \in G$ such that

$$h^{-1}gh = g'.$$

Show by example that if g and g' are conjugate, the choice of h need not be unique.

(2) Show that being conjugate defines an equivalence relation on the set G. That is, show that the relation "$g \sim g'$ if g is conjugate to g'" is an equivalence relation. Under this relation, the equivalence class of g is called the conjugacy class of g.

(3) Show that g is the only element in its conjugacy class if and only if g is in the center of G.

4.5 Conjugacy classes of Subgroups

Exercise 4.5. Let H and H' be subgroups of G. We say H and H' are conjugate if there is some g such that

$$C_g(H) = H'.$$

That is, if $gHg' = \{ghg^{-1}, h \in H\} = H'$ for some g.

(1) Show that being conjugate defines an equivalence relation on the set of all subgroups of G. That is, show that the relation "$H \sim H'$ if H is conjugate to H'" is an equivalence relation. The equivalence class of H under this relation is called the conjugacy class of H.

(2) Show that H is the only element in its conjugacy class if and only if H is normal.

Problem Sheet 5

Properties of Groups and Conjugation

5.1 Orders Revisited

Exercise 5.1. Recall that you proved any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

(1) Let $g \in G$ be an element of finite order n. Show that $g^n = 1_G$. [Hint: any element of G defines a group homomorphism from $\mathbb{Z}$.]

(2) If g is of finite order, show that the order of g is also the smallest number k for which $g^k = 1_G$. [You can use the same trick as above.]

(3) Let G be a finite group. Show that for any $g \in G$, $g^{|G|} = 1_G$.

5.2 The Opposite Group

Exercise 5.2.

(1) Given a group $G = (G, m)$, define the opposite group $G^{\text{op}} = (G, w)$ by the operation

$$w(g, h) := m(h, g).$$

That is, G^{op} as a set is the same set as G, but its multiplication happens in the opposite order. Show that G^{op} is a group.

(2) Show that the map $G \to G^{\text{op}}$ given by $g \mapsto g^{-1}$ is a group isomorphism.

5.3 Conjugation Preserves Everything

Exercise 5.3. Prove the following. Use the results form Exercise 4.2(1) and Exercise 4.3. You will have points taken off for proofs longer than 3 sentences.

(1) If g and g' are conjugate in G, they have the same order.

(2) If H and H' are conjugate subgroups in G, they have the same order.

(3) If H and H' are conjugate subgroups in G, they are isomorphic groups.

5.4 The Klein 4 Group, a Cappella

Exercise 5.4. Recall from class that $\mathbb{Z}/2\mathbb{Z}$ is a cyclic group of order 2. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (This is also written $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ sometimes.) This has the "product" group structure you studied in the last homework. This example is called the Klein four group.

(1) How many elements are in G?

(2) Show that G is not cyclic.

(3) Explain why G is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

(4) Find a subgroup of S_4 isomorphic to G. Write down the isomorphism explicitly. (Whenever you have to refer to an element of S_4, use cycle notation.)

(5) Now go Google "Klein Four Group, Finite Simple Group (of Order Two)." How many math terms do you recognize?

5.5 Index 2 Subgroups are Normal

Exercise 5.5.

(1) Let G be a group. Show that any index 2 subgroup of G is a normal subgroup. (We will later see that a group may have order divisible by 2, but still not have an index 2 subgroup.)

(2) More generally, suppose p is the smallest prime dividing $|G|$. If $H \subset G$ is a subgroup of index p, show it must be normal. [Hint: Examine the action of G on G/H. This problem will involve a few non-trivial steps.]

5.6 Orbits and Conjugation

Exercise 5.6.

(1) Let G act on a set X. Note that this defines an action of any subgroup H on X. Show that if H and H' are conjugate, then there exists a bijection ϕ between the set of orbits of the H-action, and the set of orbits of the H'-action.

(2) Using the bijection ϕ you construct, if two orbits are related by $O' = \phi(O)$, show that there is a bijection from the orbit O to the orbit O'.

Problem Sheet 6

Matrix Groups and Their Properties

6.1 Another Split Short Exact Sequence

Exercise 6.1. Let $\{\pm 1\} \subset \mathbb{R}^\times$ be the subgroup consisting of 1 and -1.

(1) Prove that
$$1 \to SO_n(\mathbb{R}) \to O_n(\mathbb{R}) \to \{\pm 1\} \to 1$$
is a short exact sequence. Here, $SO_n(\mathbb{R}) \to O_n(\mathbb{R})$ is the inclusion.

(2) Exhibit a splitting of the above short exact sequence.

6.2 $SO_2(\mathbb{R})$ is the Circle

Exercise 6.2. Recall (or convince yourself) that $SO_2(\mathbb{R})$ consists of matrices
$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$
where $a^2 + b^2 = 1$.

(1) Show that $SO_2(\mathbb{R})$ is isomorphic to the group S^1. Here, $S^1 \subset \mathbb{C}^\times$ is the subgroup of all complex numbers z such that $|z^2| = 1$.

(2) Prove that $SO_2(\mathbb{R})$ is abelian.

6.3 The Dihedral Groups

Exercise 6.3. Recall from class that for any abelian group L, the inversion $\sigma : l \mapsto l^{-1}$ defines a homomorphism
$$\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(L), \quad [0] \mapsto \mathrm{id}_L, \quad [1] \mapsto \sigma.$$
In particular, for $L = \mathbb{Z}/n\mathbb{Z}$ with $n \geqslant 2$, this defines a group
$$D_{2n} := \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}.$$
Now let $\langle x, y \rangle \subset O_2(\mathbb{R})$ be the subgroup generated by the matrix x representing rotation by $2\pi/n$ radians, and the matrix y representing reflection about the x-axis[1].

Prove that $\langle x, y \rangle$ is isomorphic to D_{2n}.

[1]The subgroup generated by means the subgroup obtained by taking all elements that are finite products of x, x^{-1}, y, y^{-1}, in any order.

Problem Sheet 7

Orthogonal Groups and Rotations

7.1 Rotational Symmetries of the Cube

Exercise 7.1.

(1) Using the orbit-stabilizer theorem, compute the number of elements in the group of rotations of $\mathbb{R}^3$ that send a perfect cube (centered at the origin) to itself. You might consider looking at faces, and not vertices.

(2) What if, instead of the cube, you consider a regular octahedron (also centered at the origin)? You should note that the regular octahedron can be drawn inside a cube, with each vertex of the octahedron at the center of a face of the cube.

7.2 Inner Product on $\mathbb{R}^n$

Recall that the dot product sends a pair $\vec{x}$, $\vec{y} \in \mathbb{R}^n$ to the real number

$$\vec{x} \cdot \vec{y} := x_1 y_1 + \cdots + x_n y_n.$$

Equivalently, if one thinks of $\vec{x}$ and $\vec{y}$ as column vectors——i.e., as $n \times 1$ matrices——we have

$$\vec{x} \cdot \vec{y} = x^{\mathrm{T}} y.$$

We say $\vec{x}$ and $\vec{y}$ are orthogonal if $\vec{x} \cdot \vec{y} = 0$. We also note that

$$\vec{x} \cdot \vec{y} = \vec{y} \cdot \vec{x} \text{ and } (t\vec{x} + \vec{x}') \cdot \vec{y} = t\vec{x} \cdot \vec{y} + \vec{x}' \cdot \vec{y}.$$

Show that the following are equivalent for an $n \times n$ matrix A:

(1) $A^{\mathrm{T}} A = I$. (i.e., $A \in O_n(\mathbb{R})$.)

(2) A preserves the dot product. That is, $A\vec{x} \cdot A\vec{y} = \vec{x} \cdot \vec{y}$ for every $\vec{x}$, $\vec{y} \in \mathbb{R}^n$. [Hint: Use that the inner product is a multiplication of a column vector and a row vector.]

(3) The columns of A are mutually orthogonal vectors of unit norm. [Hint: Every entry resulting from a matrix multiplication is a dot product of a row with a column.]

7.3 Rotations

Exercise 7.2.

(1) Let n be odd. Prove that any matrix $A \in SO_n(\mathbb{R})$ has at least one eigenvector with eigenvalue 1. [Hint: Show that $\det(A - I) = \det(I - A)$ by using the fact that $A^{\mathrm{T}}(A - I) = (I - A)^{\mathrm{T}}$.]

(2) Show that any $A \in SO_3(\mathbb{R})$ fixes a non-zero vector v, and A is rotation about this vector. [Hint: A is orthogonal, so it preserves dot products. What can you say about A's effect on the plane orthogonal to v?]

(3) By a rotation in $\mathbb{R}^3$, we mean the linear map which rotates $\mathbb{R}^3$ about some line through the origin. Show that the composition of two rotations is again a rotation (even if their axes of rotation do not agree!). Don't try to do this by computational brute froce.

So $SO_3(\mathbb{R})$ is the group of rotations in $\mathbb{R}^3$. (Likewise, you saw last week that $SO_2(\mathbb{R})$ is the group of rotations in $\mathbb{R}^2$, by seeing that $SO_2(\mathbb{R}$ is isomorphic to the circle.) This is a very special situation; in no other dimension does it hold that an element of $SO_2(\mathbb{R})$ is automatically a rotation about some axis.

(4) Show by example that $SO_4(\mathbb{R})$ has an element which does not fix any vector.

7.4 Automorphisms of a Cyclic Group

Exercise 7.3. Let C_n be a finite cyclic group of order n. (So, for instance, it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.) Let $\phi(n)$ be the number of $1 \leqslant k \leqslant n$ for which $\gcd(k, n) = 1$. ϕ is called Euler's totient function.

(1) Show that $|\mathrm{Aut}(C_n)| = \phi(n)$. [Hint: Show that an automorphism must send a generator to a generator. Then what?]

(2) Show that there are only two isomorphisms types of groups that can be obtained as a semidirect product $\mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. What are they? [Hint: What are the possible maps from $\mathbb{Z}/2\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z})$?]

Problem Sheet 8

Structure and Classification of Finite Groups

8.1 Orders and Homomorphisms

Exercise 8.1.

(1) Let $g \in G$ be an element of order n. Let $\phi : G \to H$ be a homomorphism. Show that $\phi(g)$ must be an element whose order divides n.

(2) Let G and H be finite groups. If $\gcd(|G|, |H|) = 1$, show that the only homomorphisms from G to H are trivial.

(3) Show that if $\gcd(n, m) = 1$, then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}$. [Hint: what is the order of $([1], [1]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$?]

8.2 Build-up to the Third Isomorphism Theorem

Exercise 8.2. The third isomorphism theorem answers the following question: Let's say I have a nested sequence of subgroups, $A \subset B \subset G$. Well, I could quotient out all of B to get the orbit set G/B. (In the process, all of A is divided out, too, since A is contained in B.) Or I could try to quotient out step by step: First take G/A, and then divide out by what remains of B. Is the end result the same thing? The answer is yes, and if both A and B are normal in G (so that it makes to talk about quotient groups), the end result is the same thing as groups. We'll prove this eventually. Here, you'll establish the essential pieces for proving the third isomorphism theorem.

(1) Suppose we have subgroups $A \subset B \subset G$. Exhibit an injection

$$f : B/A \to G/A.$$

[Neither of these are groups, these are just sets. After all, we haven't assumed that A is normal in G.]

(2) Let $A \subset B \subset G$ be subgroups. Suppose that A is normal in G. Prove that $A \triangleleft B$ as well. [Now it makes sense to talk about the groups G/A and B/A.]

(3) Prove that your injection f from above is a group homomorphism. This exhibits B/A as a subgroup of G/A.

(4) Exhibit a bijection

$$\psi : G/B \to (G/A)/(B/A).$$

[This just a function between two sets. To be clear, on the righthand side, we have made use of the action of B/A on G/A, since B/A is a subgroup. The quotient set $(G/A)/(B/A)$ is the usual orbit space of this action.]

(5) If G is finite, prove that

$$|G/B| = |G/A|/|G/B|.$$

8.3 Some Sylow-style Fun

Exercise 8.3.

(1) Let $G = S_3$. List all the elements of $\mathrm{Syl}_3(G)$ and $\mathrm{Syl}_2(G)$. There should be one element in the former, and three elements in the latter.

(2) In class, we showed that if $|G| = pq$ with $q > p$ primes, then G must be a semidirect product

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Assume that p does not divide $q - 1$. By considering the size of $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, and by considering Exercise 8.1(2), show that G must be isomorphic to a direct product. Conclude using 8.1(3) that G must be a cyclic group.

(3) We prove the same result a different way. Assume you don't know (and could never know) the size of $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Using the third Sylow theorem, and assuming that p does not divide $q-1$, prove that G must be a direct product $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. [Hint: How did we do this in class for $pq = 15$?]

(4) Show that any group of the following orders are cyclic:

$$65, \quad 221, \quad 9797.$$

8.4 Some Fun with Semidirect Products

Exercise 8.4.

(1) Show that there are exactly two homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to itself.

(2) Show that there are exactly two homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$. [Hint: You know how big $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ is, based on the last problem sheet. So what group must it be?]

(3) Recall that a semidirect product $L \rtimes_\phi R$ is determined by a homomorphism $R \to \mathrm{Aut}(L)$. Show that if ϕ is the dumb homomorphism (sending everything to the identity), $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

(4) If ϕ is the other homomorphism from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/3\mathbb{Z}$, show that $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong S_3$.

(5) In contrast, show that $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ must always equal $\mathbb{Z}/6\mathbb{Z}$. [The order of the semidirect product is reversed!] As a hint, you might again try to count how many elements are in $\mathrm{Aut}(L)$ for $L = \mathbb{Z}/2\mathrm{Z}$.

Problem Sheet 9

Quotients, Rings, and Modules

9.1 The Third Isomorphism Theorem for Groups

Exercise 9.1. In this problem, G need not be finite. Suppose $A \subset B \subset G$ are subgroups, and that $A, B \triangleleft G$. Building on problem sheet 8, exhibit an isomorphism

$$\psi : G/B \to (G/A)/(B/A).$$

You have proven the third isomorphism theorem. [And in case you're keeping count, don't worry——you haven't missed the second isomorphism theorem. We just haven't talked about it yet.]

9.2 Maps of Quotients

Exercise 9.2. Let A_1, A_2 and B_1, B_2 be abelian groups. Suppose we are given homomorphisms

$$\begin{array}{ccc} A_1 & \xrightarrow{i} & A_2 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ B_1 & \xrightarrow{j} & B_2 \end{array}$$

so that the above diagram commutes. This means that $gi = jf$ as group homomorphisms.

(1) Prove that the map sending $[a]$ to $[g(a)]$ is a well-defined group homomorphism from the quotient group $A_2/i(A_1)$ to the quotient group $B_2/j(B_1)$.

(2) Prove, without using any formulas involving group elements the existence and uniqueness of such a map. [Hint: Universal properties. You may use formulas involving equalities of functions, but don't ever write down elements of groups! It may help to give names to the homomorphisms $A_2 \to A_2/i(A_1)$ and $B_2 \to B_2/j(B_1)$.]

9.3 Polynomial Rings and Power Series Rings

Exercise 9.3. Let R be a commutative ring. Let $R[[x]]$ be the set of power series with coefficients in R. Explicitly, an element of $R[[x]]$ is a power series

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

We may write this as

$$p(x) = \sum_{i=0}^{\infty} a_i x^i.$$

[As you're getting used to things, it may be useful for you to think of an element of $R[x]$ as equivalent information to an ordered sequence

$$(a_0, a_1, \ldots) \in R \times R \times \cdots$$

where each $a_i \in R$.]

If p and q are two power series with coefficients a_i and b_i, respectively, we define $p+q$ to be the power series whose ith coefficient is $a_i + b_i$. That is,

$$(p+q)(x) = \sum_{i \geqslant 0} (a_i + b_i) x^i.$$

We define the product power series to have kth coefficient given by

$$\sum_{i+j=k} a_i b_j.$$

That is,

$$(pq)(x) = \sum_{k \geqslant 0} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Remark. As an explicit reminder, two power series $\sum a_i x^i$ and $\sum b_i x^i$ are equal if and only if $a_i = b_i$ for all i.

Remark. Also as a warning, note that there is no notion of convergence going on here. For instance, if the ring R is $\mathbb{Z}/n\mathbb{Z}$, there is no obvious way of talking about convergence of a power series. This is why——if you want to divorce the notion of power series in calculus from the formal algebraic manipulations we'll do here——it may help to now and then think of a power series simply as a sequence of elements of R.

(1) Prove that $R[[x]]$ is a commutative ring under the addition and product operations above.

Let $R[x] \subset R[[x]]$ be the subset of power series for which there exists some $n \in \mathbb{Z}_{\geqslant 0}$ such that $i > n \Rightarrow a_i = 0$. That is, $R[x]$ is the set of polynomials with coefficients in R.

(2) Show that the sum of two elements of $R[x]$ is again in $R[x]$, and likewise with products.

(3) Show that both the additive and multiplicative units of $R[[x]]$ are in $R[x]$.

(4) Explain why you've shown that $R[x]$ is a ring.

If $p(x)$ is not the zero polynomial, we call the largest i for which $a_i \neq 0$ the degree of the polynomial. If $p(x)$ is the zero polynomial, we will informally say that its degree is $-\infty$.

(5) Prove that $\deg(fg) = \deg f + \deg g$, with the obvious convention for what it means to add $-\infty$ to a number.

9.4 Modules as an Abelian Group with a Ring Action

Exercise 9.4. Let M be an abelian group. An endomorphism of M is a group homomorphism from M to itself. Let $\mathrm{End}(M)$ denote the set of endomorphisms from M to itself. There are two operations

$$+ : \mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M) \quad \text{and} \quad \circ : \mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M)$$

The first is defined as follows: given two endomorphisms f and g, we obtain a third endomorphism $f+g$ by declaring

$$(f+g)(x) := f(x) + g(x)$$

for all $x \in M$. The second, $\circ$, is the usual composition of functions.

(1) Show that $\mathrm{End}(M)$ is an abelian group under the operation of adding functions. That is,

(2) Let $\circ$ denote the composition of functions. Show that $(\mathrm{End}(M), +, \circ)$ is a ring.

(3) Show that an R-module structure on M is the same thing as a ring homomorphism

$$R \to \mathrm{End}(M).$$

Phiosophically, this is the same thing as saying that a group action on a set is the same thing as a group homomorphism

$$G \to \mathrm{Aut}(X).$$

There, $\mathrm{Aut}(X)$ consists of maps respects the property of cardinality of X. For modules, $\mathrm{End}(M)$ consists of maps respecting the structure of additivity of X.

Problem Sheet 10

Rings, Fields, and Modules

10.1 Fields are Very Simple

Exercise 10.1. Show that a commutative ring R is a field if and only if it only has two ideals: $\{0\}$ and R itself.

Remark. In other words, there are no meaningful quotient rings you can make out of fields——there simply aren't any interesting ideals to quotient by. So in terms of being indecomposable, this means fields are like simple groups. When one tries to use the algebra of commutative rings to study spaces, this is the reason that fields will often play the role of "points"——they are spaces that cannot be decomposed any further.

10.2 Maximal Ideals and Fields

Exercise 10.2. An ideal $I \subset R$ of a commutative ring is called maximal if the only ideal containing I is R or I itself.

(1) If I is a maximal ideal, prove that R/I is a field.

(2) Prove the converse. You may want to prove a lemma that ideals in R containing I are in bijection with ideals in R/I.

(3) Prove that $n\mathbb{Z} \subset \mathbb{Z}$ is maximal if and only if n is a prime. [Hint: Any ideal must in particular be a subgroup of $\mathbb{Z}$, and you know what all subgroups of $\mathbb{Z}$ look like.] You have shown that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

(4) In $\mathbb{Z}/7\mathbb{Z}$, verify that $\mathbb{Z}/7\mathbb{Z} - \{\bar{0}\}$ is a group by writing out its multiplication table. How does your table show that it's a group?

10.3 Field of Order 4

Exercise 10.3. From above, we learned that there is a field of order p for any prime number p. It turns out there is a field of order p^k for any prime p and any positive integer $k \geqslant 1$. We probably won't be able to prove it, except now, when $p^k = 4$.

(1) Exhibit a field $\mathbb{F}_4$ of order 4. Trial and error may be inevitable. As a hint, $\mathbb{F}_4$ is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$ as an abelian group.

(2) Let $\mathbb{F}_8$ be a field of 8 elements. [Assume it exists.] Why is $(\mathbb{F}_8 - \{0\}, \times)$ cyclic?

10.4 Direct Sum Modules and Quotient Modules

Exercise 10.4. Fix a ring R. We'll set up the idea of quotient modules and product modules, the same way we did for groups.

(1) Show that the functions

$$M \to M \oplus N, \quad m \mapsto (m, 0) \quad \text{and} \quad M \oplus N \to M, \quad (m, n) \mapsto m$$

are both left R-module homomorphisms.

(2) Let $f : M \to N$ be a homomorphism of left R-modules. Let the kernel and image of f be the kernel and image of f as a group homomorphism. Show both $\ker(f) \subset M$ and $\mathrm{im}(f) \subset N$ are submodules.

(3) Let $M' \subset M$ be a submodule, and let M/M' be the quotient abelian group. Show that the action

$$R \times M/M' \to M/M', r\overline{x} := \overline{rx}$$

makes M/M' into a left R-module.

(4) Let M and N be left R-modules. Show that $\mathrm{Hom}_R(M, N)$ is an R-module under the addition where if $f, g \in \mathrm{Hom}_R(M, N)$, then $f + g$ is defined via

$$(f + g)(x) = f(x) + g(x)$$

and for $r \in R$, the function rf is defined via

$$(rf)(x) = r(f(x)).$$

Here, x is any element of M.

10.5 The Hamiltonians/Quaternions

Exercise 10.5. We all know $\mathbb{R}^4$ is a vector space. Using an identification $\mathbb{R}^4 \cong \mathbb{R} \times \mathbb{R}^3$, let us write an element of $\mathbb{R}^4$ as

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

For historical reasons, we will write $\mathbb{H}$ instead of $\mathbb{R}^4$ in what follows.

Define a function

$$\mathbb{H} \times \mathbb{H} \to \mathbb{H}$$

by the formula

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

Here, $\cdot$ is the dot product for $\mathbb{R}^3$ and $\times$ is the cross product for $\mathbb{R}^3$.

In the following proofs, I strongly encourage you to never write out the components of $\vec{u} \in \mathbb{R}^3$.

(1) Prove that the multiplication above is associative. Verifying assoviativity requires a lot of terms, so be organized!

(2) Prove that multiplication distributes over addition of vectors.

(3) Prove that $1 := (1, (0, 0, 0))$ is the multiplicative unit.

(4) Prove by example that multiplication is not commutative.

(5) Let

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

Prove that these all square to the element

$$-1 := (-1, (0, 0, 0)) \in \mathbb{H}.$$

(6) Given an element $x = (t, \vec{v})$, let $|x|^2$ equal the usual norm-squared of a vector, so

$$|x|^2 = t^2 + |v|^2.$$

Show that $|xy| = |x||y|$. In other words, multiplication preserves the norm.

(7) Given an element $x = (t, \vec{v})$, let $\overline{x}$ denote the element $(t, -\vec{v})$. Show that any non-zero element x has a multiplicative inverse given by $\overline{x}/|x|^2$.

Remark. This ring is often called the Hamiltonians, or the Quaternions. As you proved above, it has the property that $\mathbb{H} - \{0\}$ is a group, but this ring is not a field. This is because the multiplication is not commutative. Such rings are called skew fields. When one does not demand that $R - \{0\}$ is a group, but that every non-zero element has an inverse, R is called a division rings.

Remark. You might ask, how many division rings are there? It turns out that every finite division ring must be a field. This is called Wedderburn's little theorem.

And how many division rings are there that contain the field $\mathbb{R}$ inside of them? Not many——it turns out that there are only four division rings that are vector spaces over $\mathbb{R}$:

(1) The ring with a single element, which is the zero ring.

(2) The ring $\mathbb{R}$,

(3) The ring $\mathbb{C}$, and

(4) The ring $\mathbb{H}$.

This is called the Frobenius theorem.

10.6 $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$

Exercise 10.6. As usual, in what follows, $\overline{a}$ represents the equivalence class of $a \in R$ in the quotient ring R/I.

(1) Show that $\mathbb{R}[t]/(t^2+1)$ is a vector space over $\mathbb{R}$ with basis given by $\overline{1}$ and $\overline{t}$.

(2) Show that $\mathbb{C}$ is a vector space over $\mathbb{R}$ with basis given by 1 and i.

(3) Show that there is an $\mathbb{R}$-linear map $f : \mathbb{R}[t]/(t^2+1) \to \mathbb{C}$ sending $\overline{1} \mapsto 1$ and $\overline{t} \mapsto i$. Why must this be a bijection?

(4) Show that f is a ring isomorphism.

(5) Conclude that $\mathbb{R}[t]/(t^2+1)$ must be a field.

10.7 Linear Algebra, Applied

Exercise 10.7. Let V_d be the set of polynomials in t of degree $\leqslant d$ with $\mathbb{R}$ coefficients. Fix $d+1$ real numbers a_0, a_1, …, a_d. Consider the function

$$ev_{a_0,a_1,\ldots,a_d} : V_d \to \mathbb{R}^{d+1}$$

which sends a polynomial p to the column vector

$$\begin{pmatrix} p(a_0) \\ p(a_1) \\ \vdots \\ p(a_d) \end{pmatrix}$$

(1) Show that $ev_{a_0,a_1,\ldots,a_d}$ is an $\mathbb{R}$-linear map for any choice of real numbers a_0, a_1, …, a_d.

(2) If each a_i is distinct, show that the linear map is an injection.

(3) What is the dimension of V_d?

(4) Prove that for any collection of distinct real numbers

$$(a_0, a_1, \ldots, a_d)$$

and any collection of real numbers

$$(z_0, \ldots, z_d)$$

there exists a unique polynomial p such that

$$p(a_i) = z_i.$$

(5) Fix a field F. Prove that for any collection of distinct elements

$$(a_0, a_1, \ldots, a_d), \qquad a_i \in \mathbb{F}$$

and any collection of elements

$$(z_0, \ldots, z_d), \qquad z_i \in F$$

there exists a unique degree d polynomial p with coefficients in F such that

$$p(a_i) = z_i.$$

Problem Sheet 11

Midterm Exam

11.1 Definitions

Exercise 11.1. Know the definitions of the following.

(1) Group

(2) Subgroup

(3) Order of an element

(4) Order of a group

(5) Group homomorphism

(6) Group isomorphism

(7) Kernel

(8) Image

(9) Normal subgroup

(10) Conjugation by h

(11) Conjugacy class of an element of a group

(12) $\mathrm{Aut}_{\mathrm{Set}}(X)$

(13) Group action on a set X

(14) Orbit

(15) Orbit space

(16) Index of a subgroup

(17) Stabilizer

(18) Center of a group

(19) Abelian group

(20) When H is normal, the group operation on G/H.

(21) $\mathbb{Z}/n\mathbb{Z}$

(22) S_n

(23) A_n

(24) Simple group

11.2 Normal Subgroup

Exercise 11.2. Prove that the kernel of any group homomorphism is a normal subgroup.

11.3 Cyclic Groups

Exercise 11.3. Show that if two cyclic groups have the same order (finite or not), they must be isomorphic.

11.4 Symmetric Groups and Cycle Notation

Exercise 11.4.

(1) Exhibit an explicit element τ showing that $(123)(45)$ and $(253)(16)$ are conjugate in S_6.

(2) Show that S_n has at least n distinct subgroups of order $(n-1)!$.

(3) 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.

11.5 Free Groups

Exercise 11.5.

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

(2) Prove that any finite group is finitely generated.

11.6 Simple Groups

Exercise 11.6.

(1) Show that $\mathbb{Z}$ is not simple.

(2) Show that S_3 is not simple.

(3) Show that $\mathbb{Z}/12\mathbb{Z}$ is not simple.

(4) Show that A_4 is not simple.

11.7 Index

Exercise 11.7.

(1) Let H be the subgroup of S_5 generated by $(13)(245)$. Write down every element of H.

(2) Compute the index of H inside S_5.

11.8 Theorem Statement

Exercise 11.8.

(1) State the first isomorphism theorem.

(2) State Lagrange's theorem.

11.9 The Subgroup of a Simple Group Need Not be simple

Exercise 11.9. Show by example that a subgroup of a simple group need not be simple. (You may assume that A_5 is simple.)

11.10 Group of Unit Quaternions

Exercise 11.10. 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

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

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.

11.11 Short Exact Sequences

Exercise 11.11. Show that following sequences do not split:

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

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

11.12 Chinese Remainder Theorem

Exercise 11.12. If n and m are relatively prime (meaning they share no common divisors aside from 1), show that $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(nm)\mathbb{Z}$.

11.13 Irreducibility

Exercise 11.13. 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 $f = a_d t^d + \cdots + a_1 t + a_0$ is a polynomial, we send f to

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

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

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

(2) 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.

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

(4) 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 $f(t)$?]

(5) 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?)

11.14 Principal Ideal Domains

Exercise 11.14. 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.

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

(2) 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?]

11.15 The Second Isomorphism Theorem

Exercise 11.15. Fix a group G. Let $S \subset G$ be a subgroup, and $N \triangleleft G$ be a normal subgroup.

(1) 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.

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

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

(4) 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?]

11.16 Subgroups Descend to Quotient Groups

Exercise 11.16. Let G be an arbitrary group, and $H \triangleleft G$.

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

(2) 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.

11.17 Solvable Groups

Exercise 11.17. A group G is called solvable if there exists a finite sequence of subgroups

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

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

(1) Show that any abelian group is solvable.

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

(3) 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.

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

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

11.18 $GL_n(\mathbb{F}_q)$

Exercise 11.18. Let $\mathbb{F}_q$ be a finite field with q elements.

(1) 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 $gx = y$.]

(2) 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.]

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

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

(5) 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.]

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

11.19 Ring Homomorphisms

Exercise 11.19.

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

(2) 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

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \qquad (a_{ij})(b_{ij}) = \left(\sum_{l=1}^{k} a_{il}b_{lj}\right).$$

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

$$\begin{aligned} F : M_{k\times k}(R) &\to M_{k\times k}(S), \\ (a_{ij}) &\mapsto (f(a_{ij})) \end{aligned}$$

(3) 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.

11.20 Invertible Matrices

Exercise 11.20. 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.

(1) 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 $p = 2, 3, 5$.

11.21 Bases

Exercise 11.21. Let $M = \mathbb{Z}/n\mathbb{Z}$.

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

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

11.22 Ideals are Like Normal Subgroups

Exercise 11.22. 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 $0 \in S$.)

11.23 Characteristic

Exercise 11.23. Let F be a field, and $1 \in F$ the multiplicative identity. The characteristic of F is the smallest integer n with $n \geqslant 1$ such that

$$1 + \cdots + 1 = 0$$

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 $1 + \cdots + 1$ 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.]

11.24 Solvability of S_n

Exercise 11.24.

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

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

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

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

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

Problem Sheet 12

Final Exam Practice Problems

Matrices and Cayley-Hamilton

12.1 Basics in Characteristic Polynomials

Exercise 12.1.

(1) 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 $F[t]$.

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

(3) 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.]

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

12.2 Matrices are Linear Transformations

Exercise 12.2. Let R be a commutative ring and $R^{\oplus k}$ the free module on k generators. Show there is a ring isomorphism

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

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

Remark. 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.

12.3 Some Cayley-Hamilton Applications

Exercise 12.3. Let $\mathbb{F}$ be a field of characteristic p. Let A be an upper-triangular $k \times k$ matrix with entries in $\mathbb{F}$.

(1) 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 $(-1)^{k-1}I$.

(2) With the hypothesis as in (1), prove that A is an element whose order must divide k or $2k$.

12.4 More Cayley-Hamilton

Exercise 12.4. 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 $r(A)$.

(1) 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.

(2) 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 $\Delta(t)$.

(3) Let

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

Compute A^{2014} using the methods above.

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

Rings and Ideals

12.5 Basics of Rings

Exercise 12.5.

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

(2) Give an example of a commutative ring with a zero divisor.

12.6 Prime Ideals

Exercise 12.6. 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 $y \in I$.

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

(2) 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.

12.7 Prime Ideals and Maximal Ideals

Exercise 12.7. Let R be a commutative ring.

(1) Show that every maximal ideal in R is a prime ideal.

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

12.8 A Ring that is Not a PID

Exercise 12.8.

(1) 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.

(2) Show that $\mathbb{Z}[x]$——the ring of polynomials with $\mathbb{Z}$ coefficients——is not a principal ideal domain.

Modules

12.9 $\mathbb{Z}$-modules

Exercise 12.9.

(1) Show that a $\mathbb{Z}$-module is the same thing as an abelian group.

(2) 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.

12.10 $\mathbb{Z}[t]$-modules

Exercise 12.10. 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.

12.11 Submodules

Exercise 12.11. 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 $r \in R$, $x \in N$.

(1) Show that the intersection of two submodules is a submodule.

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

12.12 Not All Modules are Free

Exercise 12.12. Give an example of a ring R and a left module M such that M is not isomorphic to a free R-module.

Computations

12.13 Computations with Matrices

Exercise 12.13. Consider the matrices

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

(1) Which of them are invertible as elements of $M_{2\times 2}(\mathbb{Z})$?

(2) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$?

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

12.14 Polynomial Roots

Exercise 12.14. Consider the polynomials

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

(1) Which of these are irreducible elements of $\mathbb{Z}/2\mathbb{Z}[t]$?

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

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

Classification of Finitely Generated PIDs

12.15 Statement

Exercise 12.15. State the classification of finitely generated modules over a PID.

12.16 Classifying Abelian Groups

Exercise 12.16.

(1) How does the theorem let us classify finitely generated abelian groups?

(2) Classify all abelian groups of order 12.

(3) Classify all abelian groups of order 16.

12.17 Another Way to Phrase Classification of Abelian Groups

Exercise 12.17.

(1) 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.

(2) 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

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

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

Groups

12.18 Your Common Mistakes

Exercise 12.18.

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

(2) Give an example of a group G, and a sequence of subgroups

$$G_1 \subset G_2 \subset G$$

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

12.19 Sylow's Theorems

Exercise 12.19. Let n_p denote the number of Sylow p-subgroups of G.

(1) Let $G = S_4$. Compute n_2.

(2) Let $G = S_4$. Compute n_3.

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

12.20 Actions and Orbit-stabilizer

Exercise 12.20.

(1) Show that $H \triangleleft G$ if and only if the normalizer of H is all of G.

(2) 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.

(3) 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.

12.21 Prove Lagrange's Theorem

Exercise 12.21. Prove Lagrange's Theorem.

12.22 Cayley's Theorem

Exercise 12.22.

(1) Show that every group acts on itself.

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

12.23 Groups of Order 8

Exercise 12.23. 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

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

(1) Show that Q is a group of order 8.

(2) Show that Q is non-abelian,

(3) Write down all subgroups of Q.

(4) Show that Q is not isomorphic to $D_{2\cdot 4} = D_8$, the dihedral group with 8 elements.

12.24 Some Big Theorems

Exercise 12.24.

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

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

is divisble by p. This is called Fermat's little theorem. [Hint: If $\mathbb{Z}/p\mathbb{Z}$ is a field, what can you say about $\mathbb{Z}/p\mathbb{Z} - \{0\}$?]

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

Terms You 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 $n \geqslant 1$ 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 Idea You Want to Know

(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 homomorphism $\phi : R \cong j(R) \to \mathrm{Aut}(L)$, 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.