H113 at Berkeley

Evan Chen
Notes from a course by Kelli Talaska

September 4, 2014

Abstract

Notes taken from Kelli Talaska's H113 (Honors Introduction to Abstract Algebra) at UC Berkeley. These notes were taken live during the lecture with TEX; particular thanks to the authors of `latexmk`. Each lecture gets its own section.

1 0117

This class will be problem-based. There will not be much lecturing, and more problem solving. We will use books all the time, but it's not strictly necessary. I think I'll just bring it every time though...

Today we will go over some preliminaries in Chapter 0- stuff we're supposed to know.

1.1 Sets and stuff (0.1)

1.1.1 Sets

You should know union, intersection, set difference, order/cardinality (size of finite set). Know Cartesian products (e.g. real plane is $\mathbb{R}^2$). Know the sets $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{C}$. This is just making sure we are using the same terminology.

1.1.2 Maps

$f : A \to B$. A is the domain, B is the codomain. Maps can be injective (one-to-one) or surjective (onto). If it's both, f is called bijective. The points that are actually hit in B are called the image. Know what an inverse image is (pre-image).

Suppose $b \in B$. Then the set which maps onto $\{b\}$ is called the **pre-image** or fiber of b.

Proposition 1.1. *Proposition 1 on page 2.*

Proof. This is my solution.

1. If f has a left inverse g, then it's obvious that f is injective since otherwise g is not a function. If f is injective, then the left inverse $g(b)$ can be defined precisely as the element $a_0 \in A$ such that $f(a_0) = b$, or arbitrarily if it doesn't exist. This a_0 is unique by injectivity. In particular, g exists.
2. Let h be the right inverse. If h exists, then $\forall b \in B : b = f(h(b))$, so h is surjective. Conversely, if f is surjective, define $h(b)$ to be any element a such that $h(a) = b$, which exists since f is surjective.

3. If f is bijective take $g = f^{-1}$. Conversely, if such a g exists, then f is injective and surjective by 1 and 2, hence bijective.
4. By definition for one direction. We claim f injective iff f surjective whenever $|A| = |B|$. This is trivial using contradiction.

□

Proof. This is Talaska's proof for (1). The definition of injective is $f(a_1) = f(a_2)$. The definition of left inverse is $\exists g$ with $g \circ f : A \to A$ is the identity. Define

$$g(b) = \begin{cases} a & \text{if } \exists a : f(a) = b \\ 1337 & \text{otherwise} \end{cases}$$

□

It's important to check that stuff is well defined. A map $f : Q \to Z$ with $f(\frac{a}{b}) = a$ is nonsense.

1.2 Equivalence Relations (0.2)

Definition 1.2. An operation $\equiv$ is an **equivalence relation** if $\forall a, b$:

- Reflexive: $a \equiv a$.
- Symmetric: $a \equiv b \Rightarrow b \equiv a$.
- Transitive: $a \equiv b, b \equiv c \Rightarrow a \equiv c$.

Such an equivalence relation partitions a set into **equivalence classes**.

Example 1.3. Parity is an equivalence relation in $\mathbb{Z}$. Formally, a b iff $a \equiv b \pmod 2$ iff $\exists n \in \mathbb{Z} : a - b = 2n$.

1.3 Modular Arithmetic (0.3)

Hey look it's $\mathbb{Z}_n$. For $n \in Z$, $a \equiv b \pmod n \Leftrightarrow n|(a-b)$. This relation splits $\mathbb{Z}$ into n equivalence classes, say $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$.

Arithmetic in equivalence classes: let A be a set with equivalence relation . Let $\oplus : A^2 \to A$ be a binary operator satisfying $\overline{a} \oplus \overline{b} = \overline{a+b}$. One needs to check that this is well defined.

Consider $\mathbb{Z}_n$. We claim that addition is well-defined mod n. Notice that

$$\bar{x} = \{x + kn | k \in \mathbb{Z}\}$$

Suppose $a_1 \equiv a_2$ and $b_1 \equiv b_2$. It's trivial to prove that $a_1 \oplus a_2 = b_1 \oplus b_2$. etc.

There's also this set $(\mathbb{Z}/n\mathbb{Z})^*$ which are the units of $\mathbb{Z}/n\mathbb{Z}$.

Exercise 1.4. Compute the remainder when 9^{1500} is divided by 100.

Solution.

$$\begin{aligned} \left(9^{10}\right)^{150} &\equiv 1^{150} \pmod{100} \\ &= 1 \end{aligned}$$

There are also some nice solutions using Binomial Theorem and some other overpowered things. □

2 0119

2.1 Groups

Definition 2.1. A **binary operation** on a set G is a map from $G^2 \to G$.

Notice that the operation does not need ot be surjective. Intuitively, a binary operation tells us how to "combine" two elements of G.

Definition 2.2. A **group** $(G, \star)$ is a set G together with a binary operation $\star$ on G satisfying

- Associativity
- Identity element: $\exists 1 \in G$ with $1 \star g = g \star 1 \, \forall g \in G$.
- Inverse: $\forall g \in G$, g has an inverse.

Hence, to verify something is a group, one needs to check that (i) The operation is a binary operation. (ii) Associativity- this usually holds because of results in $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Z}$ (iii) Identity- usu. not hard. (iv) Inverses exist.

Exercise 2.3. Exercise 6 of Section 1.1.

Solution. a) Subset of $\mathbb{Q}$ with odd denominator. (i) One can check that it's closed easily (ii) Associativity of $\mathbb{Q}$ means this is associative. (iii) Identity is 0. (iv) Inverse of x is $-x$. So it's a group.

b) $\frac{1}{2} - \frac{1}{6} = \frac{1}{3}$, so it's not closed. Hence $+$ is not a binary operation for the set, so this is not a group.

c) Not closed again. $\frac{2}{3} + \frac{2}{3} > 1$, per say. This is not a group.

d) Not closed again. $9001 - 9000.01 = 0.99$, per say. This is not group.

e) Half-integers and integers. (i) Closed under addition. Check this. (ii) Associativity follows from that of $\mathbb{Z}$. (iii) Identity is $0 = 0/1$. (iv) Inverse of x is $-x$. Hence, this is a group.

f) Not closed again. $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$, so this is not a group.

□

Here's an example of things which could go wrong.

- Is $\mathbb{Z}^+ \cup \{0\}$ a group? It's clearly closed, associative, and has identity 0, but inverses aren't in the set. This is BAD. Hence, $\mathbb{Z}^+ \cup \{0\}$ is not a group.

Note: $\mathbb{Z}^+$ is strictly positive.

Proposition 2.4. *Proposition 1 of section 1.1.*

- *The identity of a group G is unique.*
- *Each element has a unique inverse.*
- *$(a^{-1})^{-1} = a$. This is easy.*
- ***This is important!** For all a and b, $(ab)^{-1} = b^{-1}a^{-1}$. Order is important for non-commutative operations.*
- *We never bother writing parentheses since stuff is associative. Associativity for more than $n > 3$ things follows from the special case $n = 3$.*

Proposition 2.5. *(Cancellation properties) $ax = ay \Rightarrow x = y$. $xa = ya \Rightarrow x = y$.*

This follows from multiplying by a^{-1} on the left and the right, repesectively.

2.2 Class exercise

Exercise 2.6. In class, we're doing exercises 7,8,9 from 1.1.

Solution. 7. The hard part is associative. Compute

$$(x \star y) \star z = x + y - \lfloor x + y \rfloor + z - \lfloor x + y + z - \lfloor x + y \rfloor \rfloor$$
$$x \star (y \star z) = x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z - \lfloor y + z \rfloor \rfloor$$

Since $\lfloor n + x \rfloor = n + \lfloor x \rfloor \ \forall n \in Z$, it's clear that these are equal.

8. Easy. Also recall that $1 + 1 = 2$.
9. Easy. Arithmetic and use the fact that $\sqrt{2} \notin \mathbb{Q}$ so that $a^2 - 2b^2 \neq 0$ in dnominators.

□

Definition 2.7. Suppose $x \in G$. Then the order of x is the smallest positive integer n such that $x^n = 1$.

2.3 Dihedral Groups

Moving around a square.

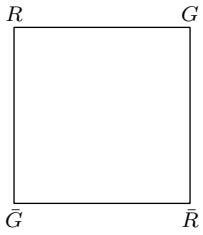

Figure 1: Red and green

What can we do with symmetry here? We do nothing. We have rotations R_{90}, $R_{180} = R_{90}^2$ and $R_{270} = R_{90}^3$. However, $R_{90}^4 = 1$. This is a group of order 4, evidently. There's also a reflection s. etc. etc. we get the dihedral group D_8.

Multiplication table of $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. D_8 is not abelian. Indeed, $sr = r^{-1}s$.

Next time, we'll have generators/relations, sym groups, matrix groups, quaternions.

3 0124

3.1 Housekeeping

Reminders:

- HW 1 is due Thursday.

  5 out of 10 problems will be graded carefully. The score will be out of 5 points for contents and 3 points for presentation. The other 5 will be scored out of two points for completion.

- Reading Check for Thursday should be here.

Today we will be discussion presentations, classic examples (symmetric groups, matrix groups, Q_8). Not in the book: Cayley graphs, which will allow us to visualize some groups.

3.2 Generators

Definition 3.1. Let S be a subset of G. We say S *generates* the group G if *every* element of G can be written as a finite product of elements in S (and their inverses).

Question. Why is the condition "and their inverses" not necessary if G is finite?

Solution. In a finite group, all elements have a finite order. Then $x^{-1} = x^{|x|-1}$. So for $x \in S$, if we want to use x^{-1} we can just use $x^{|x|-1}$ instead. This doesn't hold when G is infinite. □

Example 3.2. $\{1\}$ generates $\mathbb{Z}$. It's important that -1, the inverse of 1 is also allowed: we need it to write all integers as the sum of 1 and -1. When writing S, it's conventional to omit the inverses of S, though it doesn't make a difference.

As far as presentations, we have

$$D_{2n} = \ < r, s \,|\, r^n = s^2 = 1, rs = sr^{-1} >$$

It's common the relations are the orders of the generators. A presentation is not unique, however. This particular presentation is useful because each element can be written as $r^k s^\ell$ for $\ell \in \{0, 1\}$ and $k \in \{0, 1, \cdots, n-1\}$.

Presentations are like barycentric coordinates: for stuff they're good, they're good! But there are a lot of limitations.

Note 3.3. Some words of caution:

- The order of the group is not obvious from the presentation.
- It is not clear if the group is finite from the presentation.
- The same group can have multiple presentations which are fundamentally different.

In class, someone asked whether we needed relations if there is only one generator. The answer is yes, although there are not too many interesting groups with one generator.

Example 3.4. Consider the cyclic group of order n. It has presentation

$$\mathbb{Z}/n\mathbb{Z} = \ < \bar{1} \,|\, n \cdot \bar{1} = \bar{0} > \ \cong \ < x \,|\, x^n = 1 >$$

3.3 Classic Groups

Here are classical examples of a group.

3.3.1 Symmetric Groups

We need a definition.

Notation. Let n be a positive integer. In this class, $[n]$ will denote $\{1, 2, \cdots, n\}$.

Definition 3.5. A *permutation* is a bijection from a set (not necessarily finite) to itself. The group S_n, where n denotes the size of the set which is being permuted, is the group of bijections from $[n] = \{1, 2, \cdots, n\}$ to itself. The group operation is function composition: $\sigma \circ \tau$ will be abbreviated as $\sigma\tau$, where τ is first and σ is second.

What are the benefit of cycle notation? It makes orders and inverses immediately obvious from that representation of the element.

Example 3.6. Consider $\pi = (1\,4\,7)(2\,3)(5\,8) \in S_8$. The omission of 6 indicates that 6 is a fixed point. Conveniently, these cycles are disjoint, and only fixed points are omitted. Powers of a cycle are also not difficult: say, $(a\,b\,c\,d)^2 = (a\,c)(b\,d)$. It's also clear that the order of a cycle is a length.

In that case, we can get that $\pi^2 = (2\,3)(5\,8)$.

The above discussion yields easily.,

Proposition 3.7. *The order of a permutation written in cycle notation is the least common multiple for the lengths.*

Proof. Clear. □

3.3.2 Matrix Groups

Let F be a field. Matrix groups will consist of matrices with entries from a field. (Sidenote: Why is 0 allowed to have no inverse? This is an easy exercise.) (Sidenote 2: Why the distributive property? What motivates us to give this axiom? I didn't get a good answer to this... I'll look it up later.)

Definition 3.8. Let F be a field. Define $GL_n(F)$ be the field of $n \times n$ matrices with nonzero determinants. $*$ is matrix multiplication.

Notation. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is the group. $\mathbb{F}_p$ is the field based off of $\mathbb{Z}_p$.

Example 3.9. Consider $GL_2(\mathbb{F}_2)$. (List out the six elements of it.)

3.3.3 Cartesian Product

The Cartesian product allows us to combine two groups into another group. Personally I don't find it very interesting because it doesn't have anything "new" in it: everything is just done componentwise. It is definitely a useful notation though.

Proposition 3.10. *Let $(G, \star)$ and $(H, \cdot)$ be groups. Then $(G \times H, \star \times \cdot)$ is also a group. If we let $\triangle = \star \times \cdot$ then we have $(a, b) \triangle (c, d) = (a \star c, b \cdot d)$.*

Proof. Clear. □

3.4 Cayley Graphs

Definition 3.11. Consider a group G with a set of generators S. The *Cayley Graph* C is constructed as follows: the vertices of C are elements of G. A directed edge labeled $s \in S$ is drawn between g_1 and g_2 iff $g_1 = sg_2$.

3.5 In-Class Exercises

- Exercises 1,2,17,18 from gen/relations.
- Exercises 1,4,11 in matrix groups.
- Cayley graphs handouts.

4 0126

$\exists$ a handout on the website with some comments (under other handouts) which answers some questions that came up in class yesterday. In general, this section of the site will contain miscellaneous comments.

Also the first MUSA meeting is today at 5-7pm.

4.1 Homomorphisms and Isomorphisms

Intuitively, two groups are the "same" if they have the same structure.

Definition 4.1. A *group*[1] *homomorphism* from the groups $(G, \star)$ to $(H, \cdot)$ is a map $\phi : G \to H$ such that $\forall x, y \in G$, $\phi(x \star y) = \phi(x) \cdot \phi(y)$.

Proposition 4.2. *Let $\phi : G \to H$ be a homomorphism. Then*

1. $\phi(1_G) = \phi(1_H)$.
2. $\phi(x^{-1}) = \phi(x)^{-1}$

Proof. 1. $\phi(1 \star 1) = \phi(1) \cdot \phi(1) = \phi(1) \Rightarrow \phi(1) = 1$

2. Clear.

□

Definition 4.3. An *isomorphism* of groups G and H is a homomorphism $G \to H$ which is also a bijection.

Question. What properties of a group or its elements are preserved by isomorphism?

Some things are

1. Cardinality of the group (i.e. cardinality)
2. Cayley graphs, up to graph isomorphism (assuming the same set of generators)
3. Abelian-ness
4. Order of elements. In particular, the multiset of orders is preserved.

It's important to realize that this is necessary, but not sufficient!

This came up in class. I think it's almost certainly false.

Conjecture 4.4. *Prove or disprove: if two finite groups have the same multiset of orders, then they are isomorphic.*

On a less difficult note:

Exercise 4.5. (1.6/2) Let $\phi : G \to H$ be an isomorphism. Show that $|\phi(x)| = |x| \, \forall x \in G$.

Solution. Suppose $|x| = n$. Clearly, $\phi(x^n) = 1$, so $\phi(x)^n = 1$ Thus, $|\phi(x)| \leq n$. Suppose BWOC[2] that $\phi(x^k) = 1$ is 1 for some $1 \leq k < n$. Then $\phi(x^k) = 1$. Apply ϕ^{-1}; this is OK since $|phi$ is bijective. Then $x^k = 1$, contradiction. Thus $|\phi(x)| = n$. □

[1] This should be something that's mentioned in the book. Later on there will be ring and field homomorphisms

[2] by way of contradiction

Let $\varphi : G \to H$ be a homomorphism. Actually, we don't know anything about the relative size of G and H. We do know that $|G| \geq |\varphi(G)|$ though. What are some examples of homomorphisms?

- If $H = \{1_H\}$, then we have a trivial homomorphism.
- The identity map.
- If $\varphi : \mathbb{Z} \to \mathbb{Z}$, then some examples are $x \mapsto -x$, $x \mapsto 17x$. The former is an isomorphism, but the latter is... sort of?... an isomorphism. It's an isomorphism from $\mathbb{Z} \to 17\mathbb{Z}$ though.
- $\varphi : D_{12} \to D_6$ given by $s_{12} \mapsto s_6$ and $r_{12} \to r_6$. Check that this is a homomorphism, but not an isomorphism. Note that $|r_{12}| \neq |r_6|$. Hence the exercise above holds only for isomorphism, and not for homomorphisms. Check this works because of the presentation of D_{12} and D_6.

4.2 Group Actions

Definition 4.6. A group G *acts* on a set A if there is map $G \times A \to A$ such that (i) $g_1(g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and (ii) $1 \cdot a = a$.

How do we think of an action? If we fix $g \in G$, then we can see that $g : A \to A$ is a permutation of A. Why? If $g \cdot a = g \cdot b$, then act with g^{-1} to get $a = b$, so we have injectivity. Since this is a map from a set to itself, it is surjective and hence bijective as well (assuming A is finite, otherwise there's a bit more to check.)

Hence, the overall action is a collection of permutations of S_A, one for each $g \in G$, which may overlap. These follow the multiplication rules in our original group G.

More formally, we can think of a group action as a homomorphism from $G \to S_A$. This is called a *permutation representation* of the action.

4.3 Key Terms

- Trivial action: $g \star a = a$ for everything; that is, g is an identity permutation.
- Faithful. Every g has a different permutation of A.
- Kernel of an action. The set of g that is the identity permutation in the action.
- Left regular action. Just left multiplication when G acts on itself.

4.4 Exercises

These check to see if you know the definitions! 1.7/5, 1.7/13, 1.7/16.

5 0131

Reminders:

- Office hours tonight 6-9pm at 889 Evans
- HW 2 due Thursday. Read homework handout before turning in! Follow directions.

5.1 Subgcroups

Question. How can H fail to be a subgroup of $G = (G, \star)$?

Some ways to fail are (i) H is not a subgroup of G. (ii) H empty (or, no identity element) (iii) Multiplication for H is not same as in G. (iv) H is not closed under $\star$. (v) Inverses need to be in H. (vi) $1 \in H$.[3] among other (?) bad things.

This can be simplified into what is called the subgroup criterion.

Proposition 5.1 (Subgroup Criterion)**.** *The conditions*

- $0 \subset H \subseteq G$
- $\forall x, y \in H$, $xy^{-1} \in H$

hold if and only if $H \leq G$.

Proof. One direction is easy.

If $x = y$, we find that $1 \in H$. Then taking $x = 1$ yields $y^{-1} \in H$. Finally, suppose $a, b \in H$. Take $x = a$ and $y = b^{-1} \in H$ to get $ab \in H$. □

5.2 Centers, centralizers, and normalizers

We begin with several definitions.

Definition 5.2. The *center* of a group G, called $Z(G)$, is the set of elements $g \in G$ which commute with **all** elements of G.

Suppose we want to generalize to any $A \subseteq G$ instead of all elements.

Definition 5.3. The *centralizer* of $A \subseteq G$ is the set of $g \in G$ which commute with all elements in A.

Let's think about this in terms of actions. We want $ag = ga \forall a \in A$. This is equivalent to $g^{-1}ag = a$.

An action gives us a homomorphism $G \to S_G$. If we choose the action to be conjugation, which induces a map $\sigma_g : A \to A$. Then $g \in C_G(A)$ iff σ_g restricted to A is the identity permutation; that is, σ_g fixes elements of A.

Notice that $C_G(G) = Z(G)$.

Definition 5.4. The *normalizer* of a subset $A \subseteq G$ is the set of elements $g \in G$ such that $g^{-1}ag \in A \, \forall a \in A$.

This is equivalent to $g^{-1}Ag = A$, which can be checked by the cancellation laws.

Here, if we think of G acting on itself by conjugation, then $g \in N_G(A)$ iff the map $\sigma_g : G \to G$ if $\sigma_g | A \in S_A$.[4]

Fact 5.5. For $A \subseteq G$ nonempty, both $C_G(A)$ and $N_G(A)$ are subgroups of G, and hence also $Z(G)$.

Fact 5.6. $C_G(A) \leq N_G(A)$.

Proof. Clear. □

[3] This is a consequence of the previous statements.
[4] $\sigma_g | A$ means "σ_g restricted to A.

5.3 Stabilizers and Kernels

Suppose G acts on a set S by an action $\cdot$.

Definition 5.7. The *stabilizer* of $s \in S$ in G is the set

$$\{g \in G | g \cdot s = s\}$$

Definition 5.8. The *kernel* of the action is the intersection of the stabilizers of s as s ranges all elements of S; that is, the kernel is the set

$$\{g \in G | g \cdot s = s \, \forall s \in S\}$$

5.4 Problems to try

2.1: 5,8,11,12,14

2.2: 5,6,10

6 0202

MUSA has REUS next Thursday. Hm...

6.1 Cyclic Groups

6.1.1 Definition

Definition 6.1. A group G is **cyclic** if it has a presentation with a single generator.

Note that it suffices for such a presentation to exist. In other words, a cyclic group can have a presentation with a minimal set of generators greater than one.

For example,

$$\mathbb{Z} = \langle 1 \rangle = \langle 2, 5 \rangle$$

6.1.2 Properties

- $\exists x \in G$ such that $|x| = |G|$. [5]
- Abelian.
- Every subgroup is itself cyclic. (The converse is not true.)

There is a unique cyclic group of every size, up to isomorphism. In particular, it is isomorphic to $(\mathbb{Z}_n, +)$ if $|G| = n$ is finite, so now we can use NT.

[5] In fact, there are $\phi(|G|)$ such elements, namely $x^k \, \forall (k, |G|) = 1, 1 \leq k < |G|$.

6.2 Subgroups

Question. How can we form more subgroups of G?

Take any subset $A \subseteq G$, find the smallest subgroup of G that contains all elements in A. How do we do this?

One way is "bottom up".

- Begin with A
- Put in all the inverses of elements of A.
- Start taking products.

The other is "top down".

- Intersect all subgroups of G which contain A.

It's easy to show that the intersection of several subgroups is a subgroup; this is nonempty because $1 \in H \, \forall H \leq G$.

Groups with one generator are nice. A word of caution: groups with at least 2 generators can get pretty crazy. Be careful with presentations! It is entirely possible to construct groups with two generators of known order and end up with a group of infinite order.

6.3 Using the lattice of subgroups of G to find centralizers and/or normalizers

Fact 6.2. If $H \leq G$, then $H \leq N_G(H)$. If H is abelian, then $H \leq C_G(H)$.

This generates a useful computational corollary.

Corollary 6.3. *If $x \in G$, then $C_G(x) = C_G(\langle x \rangle)$.*

This helps compute centralizers easily given the lattice of subgroups. For example,

Example 6.4. Consider D_8. Find $C_G(r)$.

Solution. $C_G(r) = C_G(\langle r \rangle) \geq \langle r \rangle$. According to the lattice, we can get that $C_G(r) \in \{D_8, \langle r \rangle\}$. But $s \in D_8, s \notin C_G(r)$. Hence $C_G(r) = \langle r \rangle$. □

6.4 Miscellaneous exercise

Exercise 6.5 (2.3/12)**.** Show that (a) $\mathbb{Z}_2 \times \mathbb{Z}_2$, (b) $\mathbb{Z}_2 \times \mathbb{Z}$, and (c) $\mathbb{Z} \times \mathbb{Z}$ are not cyclic groups. (Groups are additive).

Solution. (a) Everything has order 2 or 1.

(b) Suppose for contradiction $(\bar{a}, b)$ is a generator. If $\bar{a} = \bar{0}$, then the first coordinate is also 0. Otherwise, we cannot hit $(\bar{1}, 2b)$.

(c) Suppose for contradiction (a, b) is a generator. Then $(a, b)^k = (ka, kb)$, so the ratio between the coordinates is invariant.

□

Exercise 6.6 (2.3/13)**.** Show that the pairs of (additive) groups (a) $(\mathbb{Z} \times \mathbb{Z}_2, \mathbb{Z})$, and (b) $(\mathbb{Q} \times \mathbb{Z}_2, \mathbb{Q})$ are not isomorphic.

Solution. (a) One is cyclic, the other isn't

(b) $\mathbb{Q} \times \mathbb{Z}_2$ has an element of order 2, while $\mathbb{Q}$ does not.

□

Here are exercises to do in groups.

Section 2.3: 9,16.

Section 2.4: 3,12,15,16

Section 2.5: 4.

7 0207

7.1 Reminders

- Thurs 5-7: Musa Undergrad
- HW2 not finished; pick up tomorrow at 12-3pm.
- See notes on HW late tonight

7.2 Quotient groups

Suppose we have a homomorphism $\varphi : G \to H$. Recall that

$$\begin{aligned} \varphi(1_G) &= 1_H \\ \varphi(x^{-1}) &= \varphi(x)^{-1} \\ \varphi(x^n) &= \varphi(x)^n \\ \Rightarrow |\varphi(x)| \mid |x| & \\ \varphi(G) &\leq H \\ \ker \varphi &\leq G \end{aligned}$$

Consider $\varphi : \mathbb{Z} \to Z_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ by $k \mapsto \bar{k}$.

Claim 7.1. These sets form a group under some multiplication (in this special case, $\mathbb{Z}/n\mathbb{Z}$). In general, this works for any surjective homomorphism $\varphi : G \to H$. We may think of these fibers (which are sets) as group elements.

$\varphi^{-1}(h_1)\varphi^{-1}(h_2) = \varphi^{-1}(h_1h_2)$ is the desired multiplication. This works because $g_1 \in \varphi^{-1}(h_1)$, $g_2 \in \varphi^{-1}(h_2) \Rightarrow \varphi(g_1g_2) = h_1h_2$.

7.3 Cosets

First, a definition.

Definition 7.2. Suppose $N \leq G$, $g \in G$. We define the *left coset*

$$gN = \{gn \mid n \in N\}$$

Fact 7.3. $g \in gN$ (since $1 \in N$).

There is a similar definition "right coset". We generally sue left cosets because the two are anologous (although in general $gN \neq Ng$.

Definition 7.4. Suppose $N \leq G$, $g \in G$. We define the right coset

$$Ng = \{ng \mid n \in N\}$$

Suppose $\varphi : G \to H$ is a homomorphism with kernel K. What do (nonempty) fibers look like? We have $K = \varphi^{-1}(1_H)$ and $1 \cdot K \Rightarrow K$ is a coset. Hence

Claim 7.5. All other fibers are of the form uK.

Proof. Let $\varphi(a) \in S$ of a coset. Then we want the elements $g \in G$ such that $\varphi(g) = \varphi(a) \Rightarrow \varphi(ga^{-1}) = 1$. This becomes $ga^{-1} \in K$, or $g \in aK$. □

Claim 7.6. the cosets of any $H \leq G$ partition G.

Proof. This is precisely the same concept that was used in the proof of Lagrange's theorem using orbits in Chapter 1. □

Claim 7.7. $uK = vK \Leftrightarrow uv^{-1} \in K$.

Proof. Clear. □

Claim 7.8. Any two distnict cosets have an empty intersection.

Proof. Suppose $\varphi(gK) = \varphi(hK)$. WTS $gK = hK$. But this is $\varphi(g) = \varphi(h) \Rightarrow \varphi(gh^{-1}) = 1$. It follows that $gh^{-1} = 1$. □

In G/K, $gK \cdot hK = (gh)K$. check that this operation is well-defined!

7.4 Exercise

Let $\varphi : D_8 \to Z_4 = \langle x^4 \mid x^4 = 1 \rangle$ be defined by

$$r \mapsto x^2, \quad s \mapsto x^2$$

The kernel of this map is

$$K = \{1, r^2, sr, sr^3\}$$

We can do a quick computation of all the elements of D_8. (Actually, for $a = r^\alpha s^\beta \in D_8$, $\varphi(a) = x^{2(\alpha+\beta)}$... but shh!)

$$\begin{aligned}\varphi(1) &= 1\\ \varphi(r) &= x^2\\ \varphi(r^2) &= 1\\ \varphi(r^3) &= x^2\\ \varphi(s) &= x^2\\ \varphi(sr) &= 1\\ \varphi(sr^2) &= x^2\\ \varphi(sr^3) &= 1\end{aligned}$$

The two relevant fibers are

$$\varphi^{-1}(1) = K = \{1, r^2, sr, sr^3\} = 1K = r^2K = srK = sr^3K$$

and

$$rK = r^3K = sK\ sr^2K = \{r, r^3, s, sr^2\}$$

$|D_8/K| = 2$ is a group of order two.

7.5 Things to keep in mind

Cosets will partition a group in general $\forall N \leq G$. However, they have a group structure iff $\exists \varphi : G \to H$ a homomorphism with $\ker \varphi = N$.

As it turns out, this occurs iff $N_G(N) = G$. We call such an H *normal* and write $N \trianglelefteq H$.

A word of caution: For a fixed N, most cosets gN aren't groups! In fact, only one is.

8 0209

8.1 Houskeeping

Today we will be going over 3.1 and 3.2. We will be delaying the content through 3.3, 3.4, 3.5. In 3.4, we will not be going over composition series.

Furthermore, the midterm is on March 1, and it will cover content up to and including chapter 4.

8.2 Exercises

Exercise 8.1 (3.1/4)**.** In G/N, prove that $(gN)^\alpha = (g^\alpha)\, N$.

Solution. Recall that the definition of $uN \circ vN = (uv)N$, fro which the conclusion follows immediately. Alternatively, consider $\varphi : G \to G/N$. Then $g \mapsto gN$. The rest is trivial. □

Exercise 8.2 (3.1/5)**.** Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$. Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Solution. Clear. As an example, take $G = \mathbb{Z}$ and $N = 42\mathbb{Z}$. Pick $g = 21$. Then $2 < \infty$. For any nontrivial group G, then G/G also works. You can also pick any non-identity element in N and the orders will be different again. □

Exercise 8.3 (3.1/8)**.** Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ by $x \mapsto |x|$. Show that ϕ is a homomorphism. Find the image of ϕ and describe the kernel and fibers of ϕ.

Solution. Since $|ab| = |a||b|$ it is obvious that ϕ is a homomorphism. Now $\phi^{-1}(a) = \{\pm a\}$ and in particular the kernel is $\phi^{-1}1 = \{\pm 1\}$. there are infinitely many cosets of two members each. □

8.3 Lagrange's Theorem

Theorem 8.4 (Lagrange's Theorem)**.** *Let G be a **finite** group and $H \le G$. Then $|H| \,|\, |G|$.*

Proof. The cosets of H partition G into k cosets, each of size $|H|$, so $k|H| = |G|$. □

Question. Is the converse true? That is, if $k \,|\, |G|$, is there necessarily a subgroup of size k?

Short answer: no. Cauchy and Sylow are possible though.

Definition 8.5. Suppose $H \le G$. The index of H in G, denoted $|G : H|$, is the number of left cosets of H in G, possibly infinite. When G is finite, the index is simply $\frac{|G|}{|H|}$.

Corollary 8.6. *If $|G| = p$, then G is cyclic.*

Proof. Consider any $x \neq 1$ in G. Then $|x|$ divides p. Hence $x = p$. Then x is a generator. □

Recall that if $H \le G$, we have $H \le N_G(H) \le G$. This is trivial since $hHh^{-1} = H \forall h \in H$ by the cancellation laws.

Question. Consider D_8 and $H = \langle 1, r^2 \rangle$. What do we know about $N_{D_8}(H)$?

We know it (i) contains H (ii) The order is 2, 4, or 8.

Proposition 8.7. *Any subgroup H of index 2 in G is normal.*

Proof. Consider $g \in G \setminus H$. The left cosets of the group are H and gH. This forces $gH = G \setminus H$. Similarly, $Hg = G \setminus H$. Hence, $gH = Hg$; hence H is normal. □

Finally, know that Cauchy's Theorem and Sylow's Theorem are true; however the full converse of Lagrange is not true.

8.4 Coset Multiplication

Definition 8.8. Let $H, K \le G$. Then $HK = \{hk : h \in H, k \in K\}$.

In general, HK is not a subgroup.

Proposition 8.9. *For all $H, K \le G$, we have*

$$|HK| = \frac{|H||K|}{|H \cap K}$$

Proof. We can write $HK = \bigcup_{k\in K, h\in H} hk = \bigcup_{h\in H} hK$. We now find conditions for when $h_1K = h_2K$ for $h_1 \neq h_2$. This occurs precisely when $h_1h_2^{-1} \in K \Leftrightarrow h_1h_2^{-1} \in H \cap K \Leftrightarrow h_1(H\cap K) = h_2(H\cap K)$. Hence the number of distinct cosets hK is the same as the number of distinct cosets $h(H\cap K)$. Furthermore, each coset has $|K|$ elements. □

Proposition 8.10. *Let $H, K \leq G$. Then $HK \leq G \Leftrightarrow HK = KH$.*

Corollary 8.11. *If H $leN_G(K)$, then $HK \leq G$.*

Proof. The given is $hK = Kh \forall h \in H$, Taking the union, we get $HK = KH$.

In particular if K is normal to G and $H \leq G$, then $HK \leq G$. □

Fact 8.12. If $HK \leq G$, then join(H, K), i.e. $\langle H, K\rangle = HK$.

Exercise 8.13 (3.2/5)**.** Let $H \leq G$ and fix $g \in G$.

a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n, then $H \leq G$.

Solution. For the first part, notice that $1 \in gHg^{-1}$. We now use the subgroup criterion. Consider $gag^{-1}, gbg^{-1} \in gHg^{-1}$. Then $(gag^{-1})(gbg^{-1})^{-1} = (gag^{-1})(gb^{-1}g^{-1}) = g(ab^{-1})g^{-1}$, completing the proof. Finally, it's clear that $|gHg^{-1}| = |H|$.

For the second part, assume not. Then $\exists g \in G$ with $gHg^{-1} \neq H$, but both the LHS and RHS are groups of the same order, yet H is supposed to be unique. □

9 0214

9.1 Reminders

Midterm exam on Thursday, March 1, during class. Drop deadline Friday?

Your midterm score will later be replaced by the larger of your score on the final and your score on the midterm. Therefore, there is no incentive to miss the midterm.

9.2 The Isomorphism Theorem

Theorem 9.1 (The First Isomorphism Theorem)**.** *If $\phi : G \to H$ is a homomorphism, then $\ker\varphi \trianglelefteq G$, and $G/\ker\varphi \cong \phi(G) \leq H$. Finally, $\phi(G) = H$ if and only if H is surjective.*

Proof. Let $K = \ker\varphi$. It's clear that $K \trianglelefteq G$. Construct the map $\psi : G/K \to \phi(G)$ by $gK \mapsto \varphi(g)$. Then life is good. □

Theorem 9.2 (The Second Isomorphism Theorem)**.** *If $A, B \leq G$, $A \leq N_G(B)$, then*

(i) $AB \leq G$

(ii) $B \trianglelefteq AB$

(iii) $A \cap B \trianglelefteq A$.

(iv) $AB/B \equiv A/(A \cap B)$.

In addition, $|AB : A| = |B : A \cap B|$.

Proof. Check each part.

(i) Last week.

(ii) We want to verify that $(ab)B(ab)^{-1} = B$, which is trivial since $A \leq N_G(B)$.

(iii) It's clear that if $A \cap B \leq A$. Consider $c \in A \cap B$. Use the fact that $c \in N_G(B)$.

(iv) The quotients on either side are sensible by the earlier two parts. Consider the map $\varphi : AB/B \to A/A(\cap B)$ given by

$$\varphi aB \mapsto a(A \cap B)$$

The cosets of the left side are of the form $(ab)B_1$, hence aB. The cosets of the right are of the form $a(A \cap B)$.

Now suppose that $a_1B = a_2B$. Then $a_1a_2^{-1} \in B, A$, so $a_1a_2^{-1} \in A \cap B$. Hence, this map is well defined, and also injective. It's also obvious that this is a homomorphism from the definition of coset multiplication. Finally, it's clear that the map is surjective, notice that for arbitrary $a(A \cap B) \in A/(A \cap B)$, we are done by the definition of the map. Hence φ is an isomorphism.

□

This is sometimes called the *diamond* isomorphism theorem.

Theorem 9.3 (The Third Isomorphism Theorem)**.** *If $H, K \trianglelefteq G$, and $H \leq K$, then $(G/H)/(K/H)$ is well-defined and isomorphic to G/K.*

Proof. First, it is easy to check $H \trianglelefteq K$ since $kHk^{-1} = H$ as $k \in K \Rightarrow k \in G$, but H is normal.

So K/H consists of the elements kH and G/H consists of elements gH, for $k \in K$, $g \in G$. Since $K \trianglelefteq G \Rightarrow gkg^{-1} \in K$, we get that $(gH)(kH)(g^{-1}H) = (gkg^{-1})H = k'H$, so $K/H \trianglelefteq G/H$.

Consider the homomorphism $G/K \to G/K$ by $gH \mapsto gK$.[6] This is well defined because if $g_1H = g_2H \Rightarrow g_1K = g_2K$ since $g_1g_2^{-1} \in H \leq K$, yay. Then we have

$$\ker \varphi = \{gH : g \in K\} = K/H$$

and we just need $\varphi(G/H) = K/H$ to finish; that is, we need to check that φ is surjective which is trivial. □

This is 'cheating" in the same way that canceling the dy's in

$$\frac{dz}{dy}\frac{dy}{dx} = \frac{dz}{dx}$$

is "cheating". It happens to work!

And finally, the *lattice* isomorphism theorem. Informally, if you want to "see" the lattice of the quotient group G/N, all you need to do is look at the part of the lattice between N and G. More precisely

Theorem 9.4 (The Fourth Isomorphism Theorem)**.** *If $N \trianglelefteq G$, $\exists$ a bijection from $\{A \mid N \leq A \leq G\}$ to the set of subgroups of G/N by $A \mapsto \bar{A} = A/N$. Then*

[6]The motivation is that the random blah is very confusing, so we want to use the first isomorphism theorem to construct a homomorphism $\varphi : G/H \to G/K$ with a kernel K/H.

- *$A \le B$ (in G) iff $\bar{A} \le \bar{B}$ (in G/N).*
- *If $A \le B$ in G then $|B : A| = |\bar{B} : \bar{A}|$.*
- $\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$.
- $\overline{A \cap B} = \bar{A} \cap \bar{B}$.
- $A \trianglelefteq B \Leftrightarrow \bar{A} \trianglelefteq \bar{B}$.

Proof. The subgroups of G/N are of the form $\{1N, a_1N, a_2N \cdots\}$. □

9.3 Simple Groups

Definition 9.5. A simple group is a group G whose only normal subgroups are G and $\{1\}$.

Applications of these simple groups are largely beyond the scope of this class.

9.4 Transpositions and the Alternating Group

Definition 9.6. In the context of symmetric groups, a **transposition** is 2-cycle.

Then we have a homomorphism $\epsilon : S_n \to \{\pm 1\}$ by the number of transpositions used to write a $\sigma \in S_n$. This is well defined; in other words, every factorization of $\sigma \in S_n$ into transpositions is invariant with respect to the parity of the number of transpositions.

It is important to realize that factorizations are not unique, even up to size. To illustrate this, notice that

$$(2\,4)(1\,3)(2\,4) = (1\,3)$$

This inspires the definition

Definition 9.7. The *alternating group* $A_n \in S_n$ is defined by

$$A_n = \{A \mid \epsilon(A) = 1\}$$

9.5 Exercises

Exercise 9.8 (3.5/3)**.** Show that S_n is generated by $\{(i\,i+1) \mid 1 \le i \le n-1\}$.[7]

Proof. It's clear that S_n is generated by the set of transpositions, and it's easy to generate any transposition by a combination of transpositions. □

Exercise 9.9 (3.5/4)**.** Show that S_n is generated by $\{(1\,2), (1\,2\cdots n)\}$.

Proof. Let $A = (1\,2)$ and $B = (1\,2\cdots n)$. Then check that

$$(j\,j+1) = B^{j-1}AB^{-j+1}$$

□

[7] Although the book doesn't mention it, these $n-1$ transpositions are called *adjacent* transpositions.

10 0216

10.1 Housekeeping

The plan for the next couple days is

- Today is 4.1,4.2
- Tues: 4.3,4.4
- Thurs: 4.5,4.6
- Tues: Review
- THURSDAY MARCH 1: MIDTERM

10.2 Group Actions

Recall the definition of a group action.

Definition 10.1. We say that a group G acts on a nonempty set A if we have a mapping $g : A \to A$ with

$$1 \cdot a = a$$
$$g_1 \cdot (g_2 \cdot a) = (g_1 g_2)a$$

It is easy to see that every action of G on A corresponds to a homomorphism $\varphi : G \to S_A$.

Definition 10.2. The **kernel** of G acting on A is the set

$$\ker \varphi = \{g \in G \mid g \cdot a \forall a \in A\}$$

Definition 10.3. The **stabilizers** of a is

$$G_a = \{g \in G \mid g \cdot a = a\}$$

Notice that the kernel can be written as $\bigcap_{a \in A} G_A$.

Definition 10.4. An action is said to be **faithful** if the $\ker \varphi = 1_G$.

Definition 10.5. An action is said to be **transitive** if $\forall a, b \in A,\ \exists g \in G : g \cdot a = b$.

Example 10.6. Consider D_8 acting on the vertices of a square $A = \{1, 2, 3, 4\}$, labeled clockwise. Let r be a 90° clockwise rotation, and let s flip across the line passing through vertices 1 and 3.

It is clear that this is an action. The kernel is 1; hence the action is faithful. Is this action transitive? Yes; even rotations suffice to send 1 to $2, 3, 4$.

As an example,

Example 10.7. Let D_8 act on $A = \{\{1, 3\}, \{2, 4\}\}$. This is an action; it is not faithful since S fixes both sets. It is transitive.

Example 10.8. Consider S_n acting on $[n]$ by $\sigma : i \mapsto \sigma(i)$. This is both faithful and transitive.

Question. Can S_n act on $\{1, 2, \cdots, n-1\}$?

Solution. Yes; every action can act on any other set by the trivial action. □

Notice that if $|G| > |S_A| = |A|!$, then the action is not faithful.

Example 10.9. S_n can act on left cosets of $\langle (1\,2\,3) \rangle$ by, say, left multiplication and conjugation. The left-multiplication action is not faithful for $n > 3$. For example, $\langle (1\,2\,3) \rangle \leq K$, where K is the kernel. In fact $K = \langle (1\,2\,3) \rangle$. We have $H \to aH$ and $H \to bH$, so we can send $aH \to bH$ for all a, b; hence this is transitive.

10.3 Orbits and Cayley's Theorem

Definition 10.10. Suppose G acts on $A \neq \emptyset$. We have the equivalence relationship

$$a \sim b \quad \text{iff } \exists g : g \cdot b = a$$

The equivalence classes are called tho **orbits**; we write the orbit containing a as

$$\mathcal{O}_a = \{g \cdot a \mid g \in G\}$$

The orbits partition A; however, unlike cosets, the orbits do not have to be the same size. Then one can verify that

$$|\mathcal{O}_a| = |G : G_a|$$

The concept of an orbit leads to Cayley's Theorem. First we need

Theorem 10.11. *Let $H \leq G$. Suppose G acts on the left cosets of H by left multiplication with induced homomorphism $\pi_H : G \to S_A$, then (i) G acts transitively, (ii) the stabilizer of $1H$ is exactly H, and (iii) $\ker \pi_H = \bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup of G residing in H.*

Proof. The first part is easy.

The stabilizer is $\{gH = H \mid g \in G\}$. If $h \in H$ then obviously this works. If $g \in G - H$ then $g \cdot 1 = g \in gH$, but $g \notin H$.

The third part is essentially rearranging the definition of $\ker \pi_H = \{g \in G \mid gxH = xH \forall x \in G\}$ into $\{g \mid g \in xHx^{-1} \forall x \in G\}$, from which the conclusion follows immediately. □

As a corollary (!) of this theorem, we obtain that

Theorem 10.12 (Cayley's Theorem)**.** *Every group G is isomorphic to a subgroup of some symmetric group. In particular, if $|G| = n < \infty$, then G sits in S_n.*

Proof. Take $H = \{1\}$ in the above theorem. Then $\ker \pi_H = 1$, where $\pi_H : G \to S_G$. This map is thus injective; then $G \cong \pi_H(G)$, its image, which is a subgroup S_G. □

11 0218

11.1 Housekeeping

- Turn HW4 back in if you want writing feedback.
- Extra credit opportunity (full details online tonight), due Thursday. Submit a true-false question for the midterm.
- Midterm one week from Thursday.

11.2 Group Action by Conjugation

Question. How big is the orbit (conjugacy class) if $a \in G$?

In general, the answer is $|G : G_a|$. In particular, if the action happens to be conjugation, we have $G_a = N_G(\{a\}) = C_G(a)$, so the size of the orbit is $|G : C_G(a)|$. (Recall we have $C_G(a)$ as shorthand for $C_G(\{a\})$.)

Proposition 11.1. *Let G act on A, and let G_a be the stabilizer of $a \in A$. Then the size of the orbit of any $a \in A$ is equal to $|G : G_a|$.*

Proof. Let $\mathcal{O}_a$ be the orbit. Also notice that $G_a \le G$ and $|G : G_a|$ is the number of left cosets of G_a. So we are now tempted to make a bijection.

Perform a map $\tau : \mathcal{O}_a \to G/G_a$ by $g \cdot a = gG_a$. One can check this is a bijection, so we're done. □

How do we partition G into conjugacy classes? Every element of the center $Z(G)$ is in its own conjugacy class; that is $\{z\}$ is a conjugacy class $\forall z \in Z(G)$. For the other conjugacy classes $K_1, K_2, \cdots, K_r$, consider $g_i \in K_i$ for $i \in [1, r]$. We now easily obtain

Theorem 11.2 (Class Equation)**.** *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

This immediately gives several nice consequences. For instance,

Theorem 11.3. *If $|G| = p^\alpha$ for $\alpha \ge 1$ and p prime, then $Z(G) \neq \{1\}$.*

Proof. By the class equation, we get

$$p^\alpha = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Notice that every term of the form $|G : C_G(g_i)|$ is a prime power. It is also not equal to 1, otherwise $g_i \in Z(G)$. In that case, taking modulo p yields

$$0 \equiv |Z(G)| \pmod{p}$$

In particular, $|Z(G)| > 1$. □

11.3 Conjugations of the symmetric group

Consider $G = S_n$. conjugation sends σ to a permutation of the same *cycle types*, which is the multiset of the lengths of the disjoint cycles. This occurs because $\tau \cdot (a_1\, a_2\, \cdots, a_n) \cdot \tau^{-1} = (\tau(a_1)\, \tau(a_2)\, \cdots \tau(a_n))$. This is easy to check: suppose $\sigma(i) = j$. Then

$$(\tau \cdot \sigma \cdot \tau^{-1})(\tau(i)) = \tau(\sigma(j))$$

from which the conclusion follows immediately.

In other words, if two elements of S_n are in the same conjugacy class. Is the converse true? Yes, because by the previous result, we just pick τ to be what we want. For example, suppose we want τ such that

$$\begin{aligned} \sigma &= (1\,2)(3\,4\,5)(6\,7\,8) \\ \tau \cdot \sigma \cdot \tau^{-1} &= (3\,5)(1\,2\,4)(6\,7\,8) \end{aligned}$$

Then let $\tau : 1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 1, \cdots$, etc.

BTW, $Z(S_n) = \{1\}$. Therefore, in S_n (for $n > 2$) there is a single conjugacy class of each cycle type. This is not true for A_n.

Fact 11.4. A_5 is simple.

Proof. Long. □

For this class, you can ignore right group actions.

11.4 Exercises

Exercise 11.5 (4.3/3a)**.** What are the conjugacy classes of $G = \mathbb{Z}_2 \times S_3$?

Solution. First, compute $Z(G) = \{(\bar{0}, 1), (\bar{1}, 1)\} = \mathbb{Z}_2 \times \{1\}$. (In general, $Z(A \times B) = Z(A) \times Z(B)$)). Okay, let's start computing.

Consider $g = (\bar{0}, (1\,2))$. Conjugation leaves the first element untouched since $\mathbb{Z}_2$ is abelian, so now we can use the results on the conjugacy classes of S_n to get orbits

$$\{(\bar{0}, (1\,2)), (\bar{0}, (2\,s3)), (\bar{0}, (3\,1))\}$$

and

$$\{(\bar{0}, (1\,2\,3)), (\bar{0}, (1\,3\,2))\}$$

and the corresponding conjugacy classes upon replacing $\bar{0}$ with $\bar{1}$. □

11.5 Automorphisms

Definition 11.6. An *automorphism* is an isomorphism from a group to itself.

It is easy to check that the set of automorphisms on G, denoted $\mathrm{Aut}(G)$, forms a group under function composition.

Consider $H \trianglelefteq G$. By definition of normality, $gHg^{-1} = H$, so we can say that G acts on H by conjugation. It turns out that each conjugation is an automorphism of H.

In other words, if $\phi : G \to S_H$ is the permutation representation of this action, then in fact $\phi(G) = \mathrm{Aut}(H)$. In fact,

$$\phi : g \mapsto \{\psi_g : H \to H \text{ by } h \mapsto ghg^{-1}\}$$

One can quickly check that ψ_g is a homomorphism.

The kernel is $\ker \phi = \{g \mid h = ghg^{-1} \forall h\} = \{g \mid hg = gh \forall h\} = C_G(H)$.

We can summarize this as

Proposition 11.7. *Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H.*

Corollary 11.8. *If $K \leq G$ and $g \in G$, then $K \cong gKg^{-1}$*

Proof. Perform a map $k \mapsto gkg^{-1}$ and checks hat this is an isomorphism. □

Exercise 11.9 (4.4/3)**.** Prove that under any automorphism of D_8, r has at most 2 possible images and s has most four possible images. Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.

Proof. By order considerations, we find that r can only map to r or r^3. s cannot map to powers of r lest it commute with r. Done. □

12 0223

12.1 Housekeeping

Reminders and information:

- No reading check or homework due for next week
- Check email and website for review tips on Friday.
- Tuesday: review time in class. Bring questions.
- Office hours next week: from 4:30PM-6:30PM on Monday, or 6PM-9PM on Tuesday.
- Midterm on Thursday (in class).

According to the teacher: "I won't be there at the midterm. I'll be in Hawaii celebrating the fact that you are taking a test".

Note 12.1. Reread Corollary 15 proof. Check that $C_G(H) = C_{N_G(H)}(H)$.

12.2 Automorphisms

Definition 12.2. An *inner automorphism* is the automorphism induced by conjugation.

Definition 12.3. H is *characteristic subgroup* of G if $\sigma(H) = H$ for all $\sigma \in \operatorname{Aut} G$.

Some properties of characteristic subgroups.

- Characteristic subgroups of G are normal in G.
- If $H \leq G$ and H is the only subgroup of order $|H|$, then H char G.
- If K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.

12.3 Nuclear Sylow

Definition 12.4. A *p-group* is a group whoso order is p^α for some integer $\alpha \geq 1$.

Definition 12.5. Suppose $|G| = p^\alpha m$ where $(p, m) = 1$. A *Sylow p-subgroup* of G is a subgroup of G with order p^α.

Let $\operatorname{Syl}_p(G)$ denote the set of Sylow p-subgroups of G, and let $n_p(G) = |\operatorname{Syl}_p(G)|$.

Theorem 12.6 (Sylow's Theorem)**.** *Let G be a group. Then*

- $\operatorname{Syl}_p(G) = \emptyset$.
- *If Q is any p-group of G, and P is a Sylow p-subgroup of G, then $\exists g \in G$ such that $Q \leq gPg^{-1}$.*
- $n_p \equiv 1 \pmod p$ *and* $n_p | m$.

As a consequence, we get the following are equivalent for $|G| = p^\alpha m$ and P a Sylow p-subgroup.

- $n_p = 1$; $\operatorname{Syl}_p(G) = \{P\}$.
- $P \trianglelefteq G$.

- P char G.
- If $X \subseteq G$ consists of elements whose orders which are powers of p, then $\langle X \rangle$ is a p-group.[8]

Fact 12.7. All Sylow p-subgroups are conjugates of each other.

Proof. This is an easy consequence of the second part of Sylow's Theorem when Q is a Sylow p-subgroup. □

12.4 A Hard-ish problem

Problem 12.8 (4.5/29)**.** If G is a non-abelian simple group of order less than 100, prove that $G \cong A_5$.

We begin bashing.

For $n = 1, 2, 3, 4, 5$ the groups are abelian. For $n = 6$, use indexing to construct a simple group (smallest prime).

$n = 7$ is prime. At $n = 8$ we have cases:

- If there is an element of order 8, then it's cyclic.
- If there is an element of order 4, there is a group of index 2.
- If all elements have order two, then it's abelian.

When $n = 9 = 3^2$ this is easy. At $n = 10$, there is a group of index 2 since by Cauchy there's a group of order 5.

So far we've used the following useful facts:

Fact 12.9. If p is the smallest prime dividing $|G|$, then any subgroup of index p is normal to G.

Fact 12.10. If $|G| = pq$ for primes p and q, then the group is not simple. (If $p \neq q$ use Sylow. If $p = q$ then either cyclic or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.)

We also have that any groups of order $2p^\alpha$ are normal (take a Sylow-subgroup and use indexes). Also, groups of order p^2q are done explicitly in the book. Then for $n \in [11, 31)$.

11	Prime
12	p^2q
13	Prime
14	semiprime
15	semiprime
16	Hi
17	Prime
18	$2p^\alpha$.
19	Prime
20	p^2q
21	semiprime
22	semiprime
23	Prime
24	
25	prime pow
26	semiprime
27	prime pow
28	p^2q
29	prime
30	book

[8] Not just a subgroup.

Oops we can kill all powers of primes by using

Fact 12.11. G non-abelian, simple implies $Z(G) = 1$.

Proof. $Z(G) \trianglelefteq G$. □

to deduce

Fact 12.12. All p-groups which are non-abelian are not simple.

Proof. Use the class equation to get $Z(G) \neq 1$. □

WARNING: If Sylow p-subgroups have order at least p^2, they may have nontrivial intersection.

	31	prime		41	prime		51	semiprime	
	32	prime pow		42	pqr		52	p^2q	
	33	semiprime		43	prime		53	prime	
	34	semiprime		44	p^2q		54	$2p^\alpha$	
Compute on.	36		and on	45	p^2q	and on	55	semiprime	and on$\sim$
	37	prime		46	semiprime		56		
	38	semiprime		47	prime		57	prime	
	39	semiprime		48			58	semiprime	
	40			49	prime pow		59	prime	
				50	p^2q		$\boxed{60}$	All your base are belong to us	

61	prime
62	semiprime
63	p^2q
64	prime pow
65	semiprime
66	pqr
67	prime
68	p^2q
69	semiprime
70	pqr

Fact 12.13. If $|G| = pqr$ with is the product of distinct primes, then G normal Sylow p-subgroup.

Proof. WLOG¡ assume $p < q < r$. Notice that $n_p \equiv 1 \pmod p$, $n_p | qr$ and cyclically, and $n_p, n_q, n_r > 1$.

Since $n_r | pq$, we have $n_r = pq$ since n_r divides neither p nor q as $n_r \geq 1 + r > p, q$. Also, $n_p \geq 1 + p$ and $n_q \geq 1 + q$. Then since all the Sylow-subgroups have trivial intersection by Lagrange, we deduce that

$$1 + (p-1)n_p + (q-1)n_q + (r-1)n_r > 1 + (p-1)(p+1) + (q-1)(q+1) + (r-1)(pq) > pqr$$

so life is good □

Let's keep morale up!

71 prime
72
73 prime
74 semiprime
75 p^2q
76 p^2q
77 semiprime
78 pqr
79 prime
80

Ok let's do some of the trickier ones.

The case $n = 56$.

Solution. $n_2 \equiv 1 \pmod 2$, $n_2|7$, so $n_2 = 7$. Similarly, $n_7 = 8$. The 7-Sylow subgroups contribute $1+6\cdot 8 = 49$ elements. Now use simple bounding. □

The case $n = 40$ is easy.

Solution. $n_5 \equiv 1 \pmod 5$ and $n_5|8$. So $n_5 = 1$, so we win. □

The case $n = 80$ is more random bounding.

Solution. $n_5 \equiv 1 \pmod 5$, and $n_5|16$, so $n_5 = 16$. In that case there are $1 + 4 \cdot 16 = 65$ elements. Now use more weak bounding. □

Left to do: 24,36,48,72.

13 0228

14th Bay Area Mathematical Olympiad.

14 0301

Midterm!

15 0306

15.1 Housekeeping

- Exams returned Thursday
- No office hours today
- HW 6 due Thursday

15.2 Direct Products

Consider $G = G_1 \times G_2 \times \cdots \times G_n$. We have

$$1_G = (1_{G_1}, 1_{G_2}, \cdots, 1_{G_n})$$

Also, $g = (g_1, g_2, \cdots, g_n) \Rightarrow g^{-1} = (g_1^{-1}, g_2^{-1}, g_n^{-1})$. Each G_i is isomorphic to $(1, 1, 1, \cdots, G_i, \cdots, 1) \trianglelefteq G$. Also

$$G/G_i \cong G_1 \times G_2 \times \cdots \times G_{i-1} \times \{1_{G_i}\} \times G_{i+1} \times \cdots \times G_n \cong G_1 \times G_2 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

You can also project onto more than one group.

In short, everything behaves as expected.

Hi.

15.3 Using direct products to generate convenient groups

In light of exercise 18 of section 5.1,

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ is an infinite group with every element having order 1 or 2

(b) $\prod_{\substack{p \text{ prime} \\ \alpha \geq 1}} \mathbb{Z}_{p^\alpha}$ has an element of order n for all finite n; furthermore every element has finite order, yet the group is infinite.

(c) $\mathbb{Z} \times \mathbb{Z}_2$ has an element of infinite order and an element of order 2. So do the multiplicative groups $\mathbb{R}$ and $\mathbb{Q}$.

(d) $\prod_{k \geq 1} S_k$ has the property that every group G is isomorphic to some subgroup of it. So is $\prod_{G \text{ finite}} G$.

(e) Let $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$. Then $G = G \times G$. Or does it? Find some other G that works in the event that it doesn't.

15.4 More on Direct Products

WARNING: A subgroup $H \leq A \times B$ might be of the form $H_A \times H_B$, for $H_A \leq A$ and $H_B \leq B$, but this is not always the case.

Exercise 15.1 (5.1/4)**.** Prove that any Sylow p-subgroup of $G = A \times B$ factors as $P \times Q$, where $P \in \text{Syl}_p(A)$ and $Q \in \text{Syl}_p(B)$.

Solution. Suppose that $|A| = p^\alpha m$ and $|B| = p^\beta k$. Then $|G| = p^{\alpha+\beta} mk$. If P_0 and Q_0 are any such Sylow p-groups, then it's obvious that $P_0 \times Q_0$ is a Sylow p-subgroup. Now the key is to recall that all Sylow p-subgroups are conjugates for each other. One can check that this preserves the form $P \times Q$. Thus the Sylow p-subgroups are of that form. □

Exercise 15.2. 5.1/5 Exhibit a non-normal subgroup of $Q_8 \times Z_4$ (note that every subgroup of each factor is normal).

Solution. Consider $\langle (j, z) \rangle$. Then the subgroup generated is $\{(j, z), (-1, z^2), (-j, z^3), 1\}$. □

15.5 Finitely Generated Abelian Groups

Definition 15.3. A group is called finitely generated if there is a finite subset A of G such that $G = \langle A \rangle$.

Theorem 15.4 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group can be written as a direct product*

$$\mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

where $r, s \geq 0$ are integers and $\{n_i\}_{i\geq 1}^s \in \{2, 3, \cdots\}^s$ satisfies $n_{i+1} | n_i$ for all $1 \leq i \leq s-1$. This composition is unique.

Definition 15.5. The above is called the *invariant factor decomposition*, and $\{n_i\}_{i\geq 1}$ are called the *invariant factors*. r is called the *free rank* of G.

Equivalently, we have

Theorem 15.6 (FTFGAG, Part 2)**.** *Every finitely generated abelian group can be uniquely written as*

$$G = \mathbb{Z}^r \times \prod_{i\geq 1} A_i$$

where $|A_i| = p_i^\alpha$, where the p_i are distinct. A_i itself can be further decomposed uniquely as $\prod_{i=1}^t Z_{p^{\beta_i}}$ where $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_t \geq 1$, $\sum_{i=1}^t \beta_i = \alpha$ is a partition.

Definition 15.7. This decomposition is called the *elementary divisor decomposition*. The integers p^{β_i} are called the *elementary divisors*.

Example 15.8. Find the possible isomorphic types of an abelian group of order 360.

Solution. Compute $360 = 2^2 \cdot 3^2 \cdot 5$.

When $p = 2$, the possible partitions correspond to $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2^3$. When $p = 3$, the possible partitions are $\mathbb{Z}_9$ and $\mathbb{Z}_3^2$. When $p = 5$, the only possible partition is $\mathbb{Z}_5$.

Okayyy bash omnomnomnom. There are $3 \cdot 2 \cdot 1 = 6$ groups. □

Finally, some closing definitions:

Definition 15.9. The *rank* of a finite abelian group of type $(t_1, t_2, \cdots, t_n)$ is n.

The *exponent* is the smallest positive integer n such that $x^n = 1 \forall n$.

Note that an invariant factor decomposition allows one to instantly compute the exponent; it's value is n_1 since $n_t | n_{t-1} \cdots | n_1$, hence the LCM of the orders of the cyclic groups is n_1. It's also obvious that one can deduce the rank instantly.

Remember that both invariant factor decompositions and elementary divisor decompositions are unique. This lets us obtain, for example, answer

Question. Determine whether $\mathbb{Z}_{600} \times \mathbb{Z}_{20}$ is isomorphic to $\mathbb{Z}_{30} \times \mathbb{Z}_5 \times \mathbb{Z}_{80}$.

The answer is no. Compute

$$\begin{aligned} \mathbb{Z}_{30} \times \mathbb{Z}_5 \times \mathbb{Z}_{80} &\cong \mathbb{Z}_3 \times \mathbb{Z}_{10} \times \mathbb{Z}_5 \times \mathbb{Z}_{80} \\ &\cong \mathbb{Z}_{240} \times \mathbb{Z}_{10} \times \mathbb{Z}_5 \\ &\ncong \mathbb{Z}_{600} \times \mathbb{Z}_{20} \end{aligned}$$

Since they are now both invariant factor decompositions.

If we feel like using elementary divisors, notice that the LHS has elementary divisors $\{8, 25, 3\} \cup \{4, 5\}$ (where these are multisets), while the RHS has elementary divisors $\{2, 3, 5\} \cup \{5\} \cup \{5, 16\}$

Exercise 15.10 (5.2/9)**.** Let $A = \mathbb{Z}_{60} \times \mathbb{Z}_{45} \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}$. Find the number of elements of order 2 and the number of subgroups of index 2.

Solution. The number of elements of order dividing 2 is $2 \cdot 1 \cdot 2 \cdot 2$ (the number of ways to choose components of order 2); subtracting the identity yields 7 elements of order 2.

Since the world is abelian, the groups of index 2 correspond to groups $G/\{1, x\}$, where $x^2 = 1$. This generates 7 subgroups of index 2. Also, a group is normal iff it is the kernel of some homomorphism; hence this gets all of them. □

Exercise 15.11. 5.2/6 Prove that any finite group has a finite exponent. Give an example of an infinite group with finite exponent. Does a finite group of exponent m always contain an element of order m.

Solution. The first part is trivial. The second part is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$. For the third part, take $m = 6$ and S_3. (Notice that the exponent is defined for non-abelian groups). □

16 0308

16.1 Housekeeping

- Tues: True-False and examples quiz, for extra exam points ($\approx$ 20 minutes).
- Homework 7 Due Thursday.

16.2 Section 5.3

There's a table of groups of small order. Yay. There are many groups of order 16 which are not abelian.

16.3 Commutators

Definition 16.1. The *commutator* of two elements $x, y \in G$ is defined by

$$[x, y] = x^{-1}y^{-1}xy$$

The commutator of two subgroups $A, B \leq G$ is defined by $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$ The commutator subgroup is defined by $G' = \langle [x, y] \mid x, y \in G \rangle$.

Fact 16.2. For any A, B subsets of G, we have $[A, B] = [B, A]$.

Proof. Notice that $[a, b] = [b, a]^{-1}$. □

Fact 16.3. $G' \trianglelefteq G$.

Vaguely, we have that

- G' is "small" if G is "almost" abelian. Actually, G' is the trivial group for abelian G. G' is "big" if G is "really non-abelian".

Just from these definitions, we obtain

Proposition 16.4. *Let G be a group. Suppose $x, y \in G$ and A, B are nonempty subsets of G, we have*

(i) $xy = yx[x,y]$

(ii) $H \trianglelefteq G \Leftrightarrow [H,G] \leq H$.

(iii) $\forall \sigma \in \mathrm{Aut}(G)$, *we have* $\sigma([x,y]) = [\sigma(x), \sigma(y)]$. *Consequently,* G' *char* G, *and* G/G' *is abelian.*

(iv) G/G' *is the largest abelian quotient group; that is, if* $\exists H \leq G : G/H$ *is abelian, then* $G' \leq H$.

(v) If φ *is any homomorphism from* G *to an abelian group, i.e.* $\varphi : G \to A$, *then* φ *factors through* G'*; that is,* $G' \leq \ker \varphi$, *and* $\exists \psi : G/G' \to A$ *a homomorphism such that the projection map* $\pi : G/G'$ *satisfies* $\psi \circ \pi = \varphi$.

Proof. We prove each part.

(i) Clear.

(ii) Compute

$$\begin{aligned} H \trianglelefteq G &\Leftrightarrow ghg^{-1} \in H \forall g \in G, h \in H \\ &\Leftrightarrow ghg^{-1}h^{-1} \in H \forall g \in G, h \in H \\ &\Leftrightarrow ghg^{-1}h^{-1} \in H \forall g \in G, h \in H \\ &\Leftrightarrow [H,G] \leq H \end{aligned}$$

as desired

(iii) The first part is easy to check from the definition of $[x,y]$. The second part follows since $\sigma(G') \in G'$, implying that G' char G. In particular, $G' \trianglelefteq G$. Now notice $(xy)G' = (yx[x,y])G' = (yx)G'$, so G/G' is abelian.

(iv) If G/H is abelian, then $(ab)H = (ba)H \forall a, b \in G$, so $a^{-1}b^{-1}ab \in H$; thus $[a,b] \in H \forall a, b \in G$. In particular, $G' \leq H$, as desired.

(v) This is fancy terminology.

□

The last part of this is largely fancy terminology. For example, the associated lattice is called a *commutative diagram*.

Proposition 16.5. *Consider* HK, *where* $H, K \leq G$.[9] *The number of ways to write each element of* HK *as a product of* $h \in H$ *and* $k \in K$ *is equal to the order of* $H \cap K$.

Proof. Consider the cosets hK. Check that two cosets intersect completely or not at all. The number of distinct cosets is $|H|/|H \cap K|$ by the work in prop 3.13 of the book. The conclusion follows immediately. □

Theorem 16.6. *If* $H, K \trianglelefteq G$ *and* $|H \cap K| = 1$ *then* $HK \cong H \times K$.[10]

In particular, if in the above, $|H||K| = |G|$, then $G = H \times K$.

Example 16.7. Show that D_{12} is a direct product of smaller groups.

Proof. Write D_{12} in its usual form. Consider $D_6 \cong \{1, r^2, r^4, s, sr^2, sr^4\}$, which is normal since it has index 2. Additionally, $\mathbb{Z}_2 \cong \{1, r^3\} = Z(D_{12})$. Notice that $|D_6 \cap \mathbb{Z}_2| = 1$, so $|D_6\mathbb{Z}_2| = 12$, which implies $D_{12} = D_6\mathbb{Z}_2$. But by the theorem, $D_6\mathbb{Z}_2 = D_6 \times \mathbb{Z}_2$.

Hence, $D_{12} \cong D_6 \times \mathbb{Z}_2$. □

[9] Recall that this is a group iff $HK = KH$.
[10] The reverse direction is trivial by order considerations.

This is the first example on page 172.

Exercise 16.8. Show[11] that $D_{16} \ncong D_8 \times \mathbb{Z}_2$.

First Proof. r is an element of order 8 in D_{16}; however, there are no elements of order 8 in D_8; hence there are no elements of order 8 in $D_8 \times \mathbb{Z}_2$. □

Second Proof. $Z(D_16) = 2$ yet $Z(D_8 \times \mathbb{Z}_2) = 4$. □

Here's a random fact.

Fact 16.9. $Z(G)$ char G.

Proof. Let ϕ be an automorphism. We wish to show that if $z \in Z(G)$, then $\phi(z) \in Z(G)$. But this is easy; we have that $zg = gz \forall g \Rightarrow \phi(z)\phi(g) = \phi(g)\phi(z)$. Now notice that ϕ is surjective, so $\phi(z)g_1 = g_1\phi(z) \forall g_1 \in G$, done. □

Exercise 16.10 (5.4/16)**.** If $K \trianglelefteq G$, then $K' \trianglelefteq G$.

Proof. Since K' char $K \trianglelefteq G$, then $K' \trianglelefteq G$. □

16.4 Tests are handed back

The high score was 85 percent. I got 83 percent. The mean was about 50 percent. gg

17 0313

17.1 Houskeeping

1. Wednesday is π day. Free pi at 1015 Evans, at around 1 PM.
2. Homework 7 is due on Thursday. Asymptote will be taught on Thursday; thankfully I already know it!
3. Special assignment over spring break: learn an addition topic, turn in a 5-10 paper.

17.2 Semidirect Products

Semidirect products allow us to construct non-abelian groups from smaller groups.

The idea is this: we wish to, given two groups H and K. We want to find some "larger" group G, which contains subgroups (isomorphic to) $\tilde{H}$ and $\tilde{K}$, such that $\tilde{H} \trianglelefteq G$ and $\tilde{H} \cap \tilde{K} = 1$.

So, we construct a set $\{(h, k) \mid h \in H, k \in K\}$, but we need a different multiplication rather than simply component-wise multiplication. We need an auxiliary fact, as follows

Fact 17.1. If $\varphi : K \to \text{Aut}(H)$ then we have a group action of K on H by

$$k \cdot h = \varphi(k)(h).$$

[11] 5.4/13 is stronger, but the proofs are essentially the same.

It's clear that this is a group action since $\mathrm{Aut}(H) \le S_H$, the symmetric group of H. Anyways, it is not hard to check that this is group action from scratch; obviously $1_k \cdot h = h$ and $k_1 \cdot (k_2 \cdot h) = (k_1 k_2) \cdot h \Leftrightarrow \varphi(k_1)(\varphi(k_2)(h)) = \varphi(k_1 k_2)(h)$, which is obvious.

So we do the following

Definition 17.2. Consider two groups H and K. Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the semidirect product is the group given φ is the group with elements in

$$\{(h,k) \mid h \in H, k \in K\}$$

with operation defined by

$$(h_1,k_1)(h_2,k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

and is denoted by $H \rtimes_\varphi K$, or just $H \rtimes K$ if φ is clear from context, or not important.

It is not hard to check that this binary operation makes $H \rtimes K$ a group. For example the identity is $(1_H, 1_K)$ and

$$(h,k)^{-1} = (k^{-1} \cdot h^{-1}, k)$$

Fact 17.3. $|H \rtimes K| = |H||K|$.

Also, $H \cong \tilde{H} = \{(h,1) \mid h \in H\}$ and $K \cong \tilde{K} = \{(1,k) \mid k \in K\}$. Furthermore, $H \cap K = 1$.

Fact 17.4. $\tilde{H} \trianglelefteq H \rtimes K$.

Proof. We simply have to check that $(g,k)(h,1)(g,k)^{-1} \in H$, which is equal to $(\text{blah}, kk^{-1}) = (\text{blah}, 1) \in \tilde{H}$. □

Fact 17.5. For all $(h,1) \in \tilde{H}$ and $(1,k) \in \tilde{K}$),[12] we have

$$(1,k)(h,1)(1,k^{-1}) = (k \cdot h, 1).$$

Proof. The rightmost component is 1. The rest is computation. First,

$$(h,1)(1,k^{-1}) = (h1 \cdot 1, k^{-1}) = (h, k^{-1})$$

so $(1,k)(h,1)(1,k^{-1}) = (1,k)(h,k^{-1}) = (k \cdot h, 1)$ as desired. □

Essentially, $\tilde{K}$ "acts" on $\tilde{H}$ by conjugation.

The choice of the symbol $\rtimes$ reflects that (i) H and K do not play symmetric roles, (ii) $H \trianglelefteq H \rtimes K$, but K is not necessarily normal.

17.3 Examples

- If $\varphi : K \to \mathrm{Aut}(H)$ is the trivial map (that is $k \cdot h = h \forall h, k$), then this is just the direct product.
- The dihedral groups are semidirect products: we have

  $$D_{2n} \cong Z_n \rtimes_\varphi Z_2 = \langle y \rangle \times \langle x \rangle$$

  with $\varphi : Z_2 \to \mathrm{Aut}(Z_n)$ by $x \mapsto (\psi : y \mapsto y^{-1})$ where $\psi : Z_n \to Z_n$. To construct an isomorphism, by order considerations, it suffices to prove that there is a surjective homomorphism from $Z_n \rtimes Z_2$ to D_{2n}. We pick $r \mapsto (y,1)$ and $s \mapsto (1,x)$; ok life is good.

[12] Dummit and Foote abbreviate this as $h \in H$, which is a really obnoxious shorthand for people like me who are just starting out.

17.4 One Last Theorem

Theorem 17.6. *Suppose. $H \trianglelefteq G$, $K \leq G$ and $H \cap K = 1$. Define $\varphi : K \to \mathrm{Aut}(H)$ by k conjugating by k. Then $HK \cong H \rtimes_\varphi K$.*

17.5 Exam Add-ons

Yay! Free points!

18 0315

Why am I so bad at AIME...

18.1 The Midterm

I received the maximum 15 points possible from the additional problems; hence my midterm score is currently 98 marks.

Here is a grading scale for the midterm, where the score is the sum of your exam score and extra problems score.

Letter Grade	Minimum Score
A	96
A-	91
B+	73
B	65
B-	58
C+	51
C	42
C-	31
F	< 20

The median score was 62 marks and the average was 63.2 marks.

18.2 Rings

Note 18.1. In this class, a ring R will always have a multiplicative identity $1 \in R$.

Definition 18.2. A *ring* R is a nonempty collection of elements with two (closed) binary operations $+$ and $\cdot$ such that

(i) $(R, +)$ is an abelian group

(ii) $(R, \cdot)$ is a monoid; that is, $\cdot$ is an associative operation, and there is an identity.

(iii) There is a distributive law: for each $a, b, c \in R$ we have

$$(a + b)c = ac + ab$$

and

$$c(a + b) = ca + cb$$

R is called *commutative* if the operation $\cdot$ is commutative.

Definition 18.3. A *zero divisor* of a ring R is a nonzero $r \in R$ such that $\exists s \in R$ with $0 \in \{rs, sr\}$ and $s \neq 0$.

Definition 18.4. A *unit* of a ring R is an element $r \in R$ such that $\exists s \in R$ with $rs = sr = 1$.

Example 18.5. In the ring $\mathbb{Z}/6\mathbb{Z}$, any nonzero element which is not ± 1 is a zero divisor (check this). That is $\bar{1}$ and $\bar{5}$ are units, while $\bar{2}$, $\bar{3}$ and $\bar{4}$ are units.

Fact 18.6. No element is both a unit and a zero divisor.

Proof. Let r be a unit. If $rs = 0$, then $r^{-1}rs = r^{-1} \cdot 0 \Rightarrow s = 0$. □

It is not true in general that any nonzero element is either a zero divisor or a unit; for example, the ring $\mathbb{Z}$ has only units ± 1 but no zero divisors.

Definition 18.7. In a *division ring*, every nonzero element has a multiplicative inverse; that is, $(R, \cdot)$ is a group.

Definition 18.8. A *field* is a commutative division ring.

Note that $GL_n(F)$ is not a ring because the sum of two invertible matrices is not necessarily invertible. Anyways, $GL_n(F)$ is the units of the $n \times n$ matrices with entries from F.

Let $M_n(F)$ denote the $n \times n$ matrices with entries from F. Let $D = \{d \in M_n(F) \mid d_{ij} = 0 \forall i \neq j\}$. Then check that

- D is a subring, but it is not a division ring.
- $D \cap GL_n(F)$ is not even a ring.
- But the subset of matrices with the same value down the diagonal is a field, isomorphic to F.

Definition 18.9. An *integral domain* is a commutative ring with no zero divisors.

Example 18.10. Any field is an integral domain. $\mathbb{Z}$ is also a field.

Now we have some stronger results.

Proposition 18.11 (Dummit/Foote Prop 7.2)**.** *Assume $a, b, c \in R$ with a not a zero divisor. Then $ac = ab$ implies either $a = 0$ or $b = c$.*

Proof. Lol factor! $a(b - c) = 0$. But a is not a zero divisor; if $a \neq 0$ we now have $b - c = 0 \Rightarrow b = c$. □

18.3 Good examples

When confronted with a "construct an example", here are some rings which are not fields to keep in mind:

- The set of $n \times n$ matrices with entries from a field.
- $\mathbb{Z}/n\mathbb{Z}$.
- $\mathbb{Z}[x]$. In addition, $\mathbb{Z}_n[x]$ has zero divisors when n is composite.

19 0320

19.1 Housekeeping

- Office hours are moved to Tue 6-7:30 and 11:30-1:00 starting in April.
- Homework 6 was scored out of 53.
- Extra homework oh noes.

19.2 Familiar examples of Rings

$\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$ are examples of rings. $\mathbb{N}$ is not a ring because the are no additive inverses. $\mathbb{Q}$ is another ring. Most of these are actually fields. $\mathbb{Z}_n$ is also a ring.

Rings of functions[13] are ring upon point-wise addition and multiplication; that is, $f+g$ and $f \cdot g$.

$M_n(R)$, the set of $n \times n$ matrices with entries from a ring R. The quadratic integer rings $\mathbb{Z}[\sqrt{D}]$, with D squarefree, is also a ring. (For example, $\mathbb{C} = \mathbb{Z}[\sqrt{-1}]$).

19.3 Larger classes of rings

Definition 19.1. Given a (multiplicative) group G and a ring R, we form the **group ring** RG, whose elements are given by as $\sum_g \in G a_g G$, where $a_g \in R$.

Essentially, group rings allow us to put an additive structure on a group.

Example 19.2. $\mathbb{Z}Q_8$ consists of "polynomials" in Q_8. The elements are of the form $c_1 + c_2(-1) + c_3 i + c_4 j + c_5 k + c_6(-i) + c_7(-j) + c_8(-k)$. Notice that $c_1 + c_2(-1) \neq c_1 - c_2$, despite what our notation may suggest.

This group ring has zero divisors: $[1-(-1)][1+(-1)] = 0$.

19.3.1 Polynomial Rings

Definition 19.3. For a commutative[14] ring R, the **polynomial ring** $R[x]$ is as expected. This is also extensible to $R[x, y, z]$, say; in general the number of variables need not be one.

What are the zero divisors of a polynomial ring? As a specific example, consider $\mathbb{Z}_6[x]$. Notice that $\mathbb{Z}_6$ has zero divisors of 2, 3, and 4; we can hence create monomials $2x^k$, etc., which are zero divisors $\forall k \in \mathbb{Z}^+$. Can we construct other zero divisors?

BTW, the units are 1 and 5, and in general, the units of a polynomial ring are just the units of the original ring.

BTW, $2x+3$ is not a zero divisor. We leave as an exercise, namely 7.2/2, that $f(x) \in R[x]$ is a zero divisor iff $\exists c \in R : c \cdot f(x) = 0$.

[13] with the same domain and range $f : A \to B$. B must be a ring, but the functions need not be surjective.
[14] It is possible to make this definition for non-commutative R, but the commutative case is more interesting.

19.4 Matrix Rings

Definition 19.4. A **matrix ring** is a square $n \times n$ matrix[15] with addition and multiplication as expected.

Can we find some units? It is not hard to check that a matrix with varying units of R and along the diagonal and zero elsewhere is a unit.

Hood claims that it's necessary and sufficient that the determinant is a matrix. Anyways, $\varphi : M_n(R) \to R$ by $A \mapsto \det A$ is a homomorphism. It's obvious now that $\det A \in R^*$ is necessary. I can't tell at a glance whether this is sufficient because I know nothing about matrices; zzz linear algebra.

How about zero divisors? In a diagonal matrix, if $\det A$ is a zero divisor, then multiply by another conveniently chosen diagonal matrix to get the 0 matrix. Of course, we can extend this to lower-triangular matrices, since this doesn't change anything when one multiplies by the same conveniently chosen diagonal matrix.

19.5 More Examples

Formal power series rings: we write $R[[x]]$ as formal power series. These are basically infinite polynomials. More specifically, YAY GENERATING FUNCTIONS!

We don't care that much about convergence here. Anyways,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

19.6 Definitions

In the homework, one will find

Definition 19.5. The **center** of R, denoted $Z(R)$, is the set

$$\{z \in R \mid rz = zr \forall r \in R\}$$

Is this a subring? Check that

- $0, 1 \in Z(R)$
- One can verify $a, b \in Z \Rightarrow a - b \in Z$ by distributive laws, so this is an additive group.
- $a, b \in Z \Rightarrow ab \in Z$ holds easily.

Definition 19.6. An element x of a ring R is **nilpotent** if $x^k = 0$ for some $k \in \mathbb{Z}^+$.

Example 19.7. A nilpotent element is

$$\begin{bmatrix} 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \end{bmatrix} \in M_4(R)$$

since each "diagonal" disappears as k increases.

Example 19.8. In $\mathbb{Z}_{p^\alpha}$ for primes p, any zero divisor is nilpotent.

[15] The matrices need to be square for multiplication to work

20 0322

20.1 Housekeeping

Reminders: the office hours are now 11:30am to 1pm, and 6:00 to 7:30pm.

Next homework and reading check posted; next week.

Soon, there will be a handout on the website with modified ring definitions and theorems, since we only consider rings with a multiplicative identity.

20.2 Ring Homomorphisms

Definition 20.1. Let R and S be rings. A map $\varphi : R \to S$ is a **ring homomorphism** if

- $\varphi(a+b) = \varphi(a) + \varphi(b)$.
- $\varphi(ab) = \varphi(a)\varphi(b)$.
- $\phi(1_R) = 1_S$ if φ is nontrivial.

The third property can be derived by setting $a = 1_R$ in the second property.

Definition 20.2. Let $\varphi : R \to S$ be a homomorphism; then the **kernel** is $\ker \varphi = \{r \in R \mid \varphi(r) = 0_S\}$.

Definition 20.3. If a ring homomorphism is also bijective, then it is a **ring isomorphism**.

Note 20.4. The trivial ring $\{0\}$ has $0 = 1$. In all other rings, $0 \neq 1$.

Example 20.5. Consider the reduction map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $x \mapsto barx$ modulo n. This is a ring homomorphism.

Finally, we define the concept of an *ideal*, the analog of normal groups.

Definition 20.6. Let R be a ring, and let $I \subseteq R$. Then I is an **left ideal** if

(i) $(I, +)$ is an additive subgroup, which is equivalent to $a, b \in I \Rightarrow a - b \in I$.

(ii) I is closed under multiplication; that is, $a, b \in I \Rightarrow ab, ba \in I$.

(iii) I is closed under left multiplication by elements of R. That is, $a \in I, r \in R \Rightarrow ra \in I$.

Similarly, a **right ideal** satisfies all the conditions with "left multiplication" replaced by "right multiplication". if I is both a left and right ideal of R, then it is an **ideal** of R, sometimes termed a 2-sided ideal for emphasis.

Note 20.7. For us, since every ring has a multiplicative identity 1, the only ideals of R that are also a subring of R are the whole ring R, and the trivial ring $\{0\}$.

We can now deduce a (modified) proposition 5 in the book; that is,

Proposition 20.8 (Modified Prop 5)**.** *Suppose $\varphi : R \to S$ is a ring homomorphism. Then the image $\varphi(R)$ is a subring of S, and $\ker \varphi$ is an ideal.*

20.3 Quotient Rings

The motivation for introducing the concept of an ideal is the attempt to define quotient rings in the same way we define quotient groups. We would want R/I to not only be an additive group, but also a multiplication structure.

Let $\varphi : R \to S$ take $a \to 0$. then $ra \to 0$ and $ar \to 0$, implying the nice ideal property of $\ker \varphi$.

It turns out that R/I has a nicely defined structure (with $(r+I) \oplus (s+I) = (r+s)+I$ and $(r+I) \otimes (s+I) = (rs+I)$, so that we can just pick representatives) if and only if I is an ideal. Evidently this is not hard to check.

20.4 Isomorphism Theorems

We can now deduce the analogs of the isomorphism theorems for groups.

The heart of our work above is encoded in the first isomorphism theorem.

Theorem 20.9 (The First Isomorphism Theorem for Rings)**.** *If $\varphi : R \to S$ is a ring homomorphism, then*

(i) $\ker \varphi$ *is an ideal of R, say I.*

(ii) The cosets of I, namely $r + I$,[16] *have a ring structure given by $(r + I) + (s + I) = (r + s) + I$ and $(r + I)(s + I) = (rs + I)$.*[17]

(iii) $R/I \cong \varphi(R)$; that is, the quotient is isomorphic to the image of φ, which is a subring of S.

(iv) If I is any ideal of R, then the natural projection map $\pi : R \to R/I$ by $r \mapsto r + I$ is a homomorphism. Also, $\ker \pi = I$.

Theorem 20.10 (The Second (Diamond) Isomorphism Theorem for Rings)**.** *Let R be a ring, S a subring of R, and I an ideal of R. Then*

$$S + I = \{s + i \mid s \in S, i \in I\}$$

is a subring of R, Also, I is an ideal of $S + I$, $S \cap I$ is an ideal of S and

$$(S + I)/I \cong S/(S \cap I).$$

Proof. First, we show that $S + I$ is a ring. Clearly $S + I$ is an additive group. Also, $(s + i)(s' + i') = ss' + (is' + si' + ii')$ which is of the form $s + i$. Now obviously I is an ideal of S since it is an ideal in the larger set R. Next, it is evident that $S \cap I$ is an ideal of S.

Finally, we need to show that these are isomorphic. These are isomorphic as groups, so we need only show that the map is multiplicative, which is evident from the multiplication in quotient rings. □

We now need to define the quotient of two ideals in preparation for the third isomorphism theorem.

Definition 20.11. Let I and J be ideals of R. Let J/I be the set $\{j + I \mid j \in J\}$ equipped with the operations as usual.

Fact 20.12. J/I is an ideal of R/I.

Proof. Notice that $(r + I)(j + I) = rj + I$, but $rj \in J$ since j is an ideal. The closure of multiplication is the special case $r \in J$. The rest is trivial. □

[16] Not rI, which is pretty useless since $rI = I$.
[17] We can "distribute" $(r + I)(s + I) = rs + Is + rI + I^2 \approx rs + I$.

Theorem 20.13 (The Third "Chain Rule" Isomorphism Theorem for Rings)**.** *Suppose R is a ring, and $I \subseteq I$ are ideals of R. Then*

$$(R/I)/(J/I) \cong R/J$$

is a well-defined congruence.

Proof. As above, these quotients make sense. Now check stuff. □

Theorem 20.14 (The Fourth (Lattice) Isomorphism Theorem for Rings)**.** *Suppose I is an ideal of a ring R. Then there is a bijection $A \leftrightarrow A/I$, where A consists of the subrings of R containing I, while A/I ranges over the subrings of R/I, which preserves everything. Also, we can biject $J \leftrightarrow J/I$, where J ranges over the ideals of R containing I, and J/I ranges over the ideals of R/I.*

20.5 Exercises

Exercise 20.15 (7.3/2)**.** Show that $\mathbb{Z}[x] \ncong \mathbb{Q}[x]$.

Proof. The units of $R[x]$ are precisely the units of R. Hence, the units of $\mathbb{Z}[x]$ are $\mathbb{Z}^*$, while the units of $\mathbb{Q}[x]$ are $\mathbb{Q}^*$. But $\mathbb{Z}^* \ncong \mathbb{Q}^*$, by order considerations. □

Exercise 20.16 (7.3/3)**.** Find all homomorphic images of $\mathbb{Z}$.[18]

Solution. Alternatively, it suffices to find all ideals of $\mathbb{Z}$. Let I be any ideal of $\mathbb{Z}$. Clearly $I = \{0\}$ and $I = \mathbb{Z}$ work; so does $I = n\mathbb{Z}$.

We want to show that there are no other ideals. Suppose $k \in \mathbb{Z}$ have minimal absolute value, with $k \neq 0$. This is possible whenever $I \neq \{0\}$. Then nk must be in I for all n; hence $I = k\mathbb{Z}$, since k was minimal.

These correspond to the images $\mathbb{Z}$, $\{0\}$, and $\mathbb{Z}/n\mathbb{Z}$. □

Exercise 20.17 (7.3/4)**.** Find all ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$.

Solution. Let ϕ be a homomorphism. According to our definition, $\phi(1) = 1$ if ϕ is nontrivial. Then everything else is forced. gg. □

Exercise 20.18 (7.3/6)**.** Decide whether the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$.

(a) Projection onto the $1, 1$ entry.

(b) The trace of the matrix.

(c) The determinant of the matrix.

Solution. (a) No, since multiplication doesn't work. BTW, the diagonal matrices D are a subring of $M_2(\mathbb{Z})$, and in this case, the map is a homomorphism from D to $\mathbb{Z}$.

(b) No, since the identity matrix has a trace which is not 1.

(c) Yay the determinant is multiplicative. But it's not even a group homomorphism. How disappointing.

□

[18] i.e. what are all possible images of a φ, if $\varphi : \mathbb{Z} \to R$?

21 0403

21.1 Housekeeping

- Special assignment topics due tonight
- HW9 due next week...

21.2 Generating Ideals

Definition 21.1. Let A be a subset of a ring R. Then (A) is the (two-sided) ideal generated by A; i.e. the the smallest (two-sided) ideal containing A. RA is the left ideal generated by A, and AR is the right ideal generated by A.

Fact 21.2. $RA = \{\sum ra \mid r \in R, a \in A\}$ is the set of finite combinations of the form ra, and similarly for ar. Also,

$$(A) = RAR\ \{\sum ras \mid r, s \in R, a \in A\}.$$

Definition 21.3. An ideal is *principal* if it is generated by a single element; i.e. $I = (a)$. I is *finitely generated* if it has a finite generating set; i.e. $I = (a_1, \cdots, a_k)$.

Fact 21.4. Suppose R is commutative. Then a principle ideal $I = (a)$ is precisely the elements of the form ras, or even ra or ar, rather than finite sums. This is "very" un-true for non-commutative R– we really need the finite sums.

Example 21.5. Some examples of (possibly) principal ideals.

- For any R
  - R itself is equal to (u) for some unit $u \in R$. In particular, $R = (1)$. $\{0\} = (0)$ *is also a principle ideal.*
- Ideals in $\mathbb{Z}$
  - All ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z} = (n)$; in particular, they are all principal.
- Ideals in $\mathbb{Z}[x]$.
  - (x) is the principal $\{p(x) \in \mathbb{Z}[x] \mid p(0) = 0\}$
  - $(x, x^2) = (x)$ is the same ideal.
  - $(x, 2)$ is the set of all polynomials with even constant terms. It is *not* principal, although it is finitely generated; see below.

Claim 21.6. $(x, 2)$ is not principal in $\mathbb{Z}[x]$.

Proof. Suppose for contradiction that $I = (x, 2) = (q)$. Since $2 \in I$, $q(x)$ must be a constant polynomial. In particular, $q(x) \in \{\pm 1, \pm 2\}$. Since $\pm 1 \notin I$, we find that $q(x) \in \{\pm 2\}$. So $(q) = (-q(x))$, we may assume that $q = 2$. But now $x \in I$, yet $x \notin (q)$, which is a contradiction. □

Note 21.7. The last part uses the fact that $\nexists f \in \mathbb{Z}[x]$ such that $x = 2f(x)$.

Proposition 21.8. *Let I be an ideal of a ring R. Then*

(i) $I = R \Leftrightarrow u \in I$ for some unit u.

(ii) For commutative R, then R is a field if and only if R has exactly two ideals, namely $\{0\}$ and R.

Proof. (i) One direction is obvious. If $u \in I$, then $u^{-1}u = 1 \in I$, which yields $I = R$.

(ii) If R is a field, then let $I \neq \{0\}$ be an ideal of R. Since in a field, everything is commutative, then by the previous part, we get $I = R$. On the other hand, suppose we have only two ideals in R. Suppose $r \in R$ is nonzero. We will prove that r is a unit. Consider the ideal (r). It is not $\{0\}$, so it is R, hence by the previous part, u is a unit.

□

Corollary 21.9. *Let $\varphi : F \to R$ be a ring homomorphism, where F is a field and R is a ring. Either φ is the 0 map or φ is injective.*

Proof. Kernels are ideals, so $\ker \varphi \in \{\{0\}, R\}$. The conclusion follows. □

21.3 Maximal Ideals

Definition 21.10. An ideal $M \neq S$ in a ring S is a *maximal ideal* if the only ideals containing M are M and S; i.e. there are no ideals "in between".

Fact 21.11. All nontrivial rings R (with 1) have maximal ideals, and every ideal of R is contained in a maximal ideal.

Proof. Evidently Zorn's Lemma destroys this. □

Proposition 21.12. *If R is commutative, then M is a maximal ideal if and only if R/M is a field.*

Proof. Since M is an ideal, R/M is a well-defined field. Using the lattice isomorphism theorem, the ideals of R containing M can be bijected to the ideals of R/M by

$$I \mapsto I/M$$

Now notice that R/M is a field if and only if R/M has the two ideals $\{0\} = M/M$, and R/M, which correspond to M and R by this map. □

Note 21.13. $\{0\}$ is a maximal ideal of commutative R if and only if R is a field.

21.4 Prime Ideals

Definition 21.14. Let R be a commutative ring. An ideal $P \neq R$ of R is *prime ideal* if

$$ab \in P \Rightarrow (a \in P) \vee (b \in P) \forall a, b \in R$$

Motivation. Let $R = \mathbb{Z}$. Then the prime ideals of $\mathbb{Z}$ are precisely $p\mathbb{Z}$, where p is a prime.

Remember that everything is commutative here!

Proposition 21.15. *P is a prime ideal of R if and only if R/P is an integral domain.*

Before presenting a proof, we state a corollary.

Corollary 21.16. *Every maximal ideal M is prime.*

Proof. R/M is a field, which is therefore an integral domain, implying that M is a prime ideal. □

Returning to the main proposition,

Proof. $P \neq R \Leftrightarrow R/P \neq \{0\}$. Also

$$(ab \in P \Rightarrow a \in P \vee b \in P) \Leftrightarrow (\bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = 0 \vee \bar{b} = 0)$$

completing the proof. □

21.5 Examples of Ideals

Example 21.17. When $R = \mathbb{Z}$, the prime ideals $p\mathbb{Z}$ are precisely the maximal ideals; this is not hard to check.

Example 21.18. Take $R = \mathbb{Z}[x]$ and take the ideal (x). Then check that $R/(x) \cong \mathbb{Z}$ by the map $f(x) \mapsto f(0)$. $\mathbb{Z}$ is not a field, but it is an integral domain; hence, $R/(x)$ is prime, but not maximal.

On the other hand, $R/(2,x) \cong \mathbb{Z}_2$ by $f(x) \mapsto f(0) \pmod 2$, which is a field, so $(2,x)$ is both maximal and prime. This holds in general for any prime in place of 2.

21.6 Exercise(s)

Exercise 21.19 (7.4/16)**.** Let $E = \mathbb{Z}[x]$, and consider $E/(x^4 - 16)$.

(a) Find a polynomial of degree at most 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $x^4 - 16$.

(b) Prove that $x \bar{-} 2$ and $x \bar{+} 2$ are zero divisors in E.

Solution. (a) Long division is feasible but painful. Notice that $x^4 \equiv 16$, so we can just substitute. The answer turns out to be $-2x^3 + 25936x + 3$.

(b) Note that $(x^2+4)(x-2)(x+2) = x^4 - 16 \equiv 0$ so we're done.

□

22 0405

22.1 Reminders

THree weeks of class remain, plus RRR and finals week.

FINAL EXAM
Friday May 11, 7-10 PM
101 LSA Building

22.2 Euclidean Domains

Definition 22.1. A *norm* is on an integral domain R is a function $N : R \to \mathbb{N}$ (where $0 \in \mathbb{N}$) such that $N(0) = 0$. The norm is called a *positive norm* $N(\alpha) \in \mathbb{Z}^+ \forall \alpha \neq 0$.

Example 22.2. Absolute value is a norm for $R = \mathbb{Z}$.

Definition 22.3. An integral domain is a *Euclidean domain* if there is a norm N that yields a "division algorithm"; that is

$$\forall n, d \in R, d \neq 0 : \exists q, r \in R : a = qb + r, N(r) \leq N(d) \text{ or } r = 0$$

The motivation for this "division algorithm" is that, by repeatedly applying this, we can get a sort of "Euclidean Algorithm", which will yield a "greatest common divisor".

22.3 GCD's

Let us clearly define the concept of gcd:

Definition 22.4. For a commutative ring R and $a, b \in R$ with $b \neq 0$,

(i) a is a *multiple* of B if $a = xb$ for some $x \in R$. We may write $b|a$ for "b divides a".

(ii) For $d \neq 0$, d is *greatest common divisor* of a and b if

(1) $d|a$ and $d|b$

(2) If $d'|a$ and $d'|b$, then $d'|d$.

Note that this definition does not imply d is unique.

Can we rephrase this in terms of ideals? The conditions become

(1) $(a, b) \subseteq (d)$.

(2) $(a, b) \subseteq (d') \Rightarrow (d') \subseteq (d)$.

In other words, (d) must be the smallest principle ideal containing (a, b). In fact, in Euclidean domains, we will show that all ideals are principal, so that equality occurs; that is, $(a, b) = (d)$.

22.4 The Euclidean Algorithm

The Euclidean Algorithm for $a = 13$ and $n = 20$. This is exercise 8.1/2a.

$$\begin{aligned} 20 &= 13 \cdot 1 + 7 \\ 13 &= 7 \cdot 2 + (-1) \\ 7 &= (-1) \cdot (-7) \end{aligned}$$

Hence the GCD is 1. Note that these numbers are not unique; since we are working in $\mathbb{Z}$ and the norm is simply the absolute value, the first step could also read $20 = 13 \cdot 2 + (-6)$. The troll second step illustrates this.

Hence a GCD is -1.

Now we want to compute the numbers in Bezout...

$$\begin{aligned} -1 &= 13 - 7 \cdot 2 \\ &= 13 - (20 - 13 \cdot 1) \cdot 2 \\ &= 3 \cdot 13 - 2 \cdot 20 \end{aligned}$$

Hence taking modulo 20 we obtain $3 \cdot 13 \equiv -1 \pmod{20}$. We can then compute $13^{-1} \equiv -3 \pmod{20}$.

22.5 GCD's in Euclidean Domains

Theorem 22.5. *Every ideal in a Euclidean domain is principal.*

Proof. The idea is to show that $(a, b) = (d)$, where d is the GCD.

Assume we have a nonzero ideal I (since the zero ideal is principal). Because R is a Euclidean domain, we can execute the Euclidean algorithm for some norm N.

Consider the set $S = \{N(\alpha) \mid \alpha \in I \setminus \{0\}\} \subseteq \mathbb{N}$. Per well-ordering, $\exists d \in I \setminus \{0\}$ such that $N(d) \in S$ is minimal.

We claim that the ideal is generated by d. For any $x \in I$, invoke the division algorithm to get $x = dq + r$, where $N(r) < N(d)$ or $r = 0$. Also, $r = x - dq \in I$. But $N(d)$ is minimal; this forces $r = 0$, so x is in fact a multiple of d.

This shows $I \subseteq (d)$, while $(d) \subseteq I$ is trivial since $d \in I$. We conclude that $I = (d)$. □

22.6 Examples

We showed that $(2, x)$ is not principal in $\mathbb{Z}[x]$, although it is principal in $\mathbb{Q}[x]$. It is also principal in $R[x]$, where R is the subset of $\mathbb{Q}$ with denominators which are power of 2. The latter two are trivial since 2 is a unit in both.

$(2, x)$ is also principal in $\mathbb{Z}_{2k+1}[x]$ for $k > 0$.

In summary: context is important!

Examples of integral domains which are not Euclidean:

- $\mathbb{Z}[x]$ since there is a non-principal ideal $(2, x)$, making it impossible for it to be Euclidean.
- $\mathbb{Z}[\sqrt{-5}]$ and some (most?) other quadratic integer rings.

22.7 Miscellany

Proposition 22.6. *Let R be a commutative ring. If $a, b \neq 0$ and $(a, b) = (d)$, then d is a GCD of of a and b.*

Proof. See the proof of the earlier theorem. □

Proposition 22.7. *Let R be an integral domain. If $(d) = (d')$ for some $d, d' \in R$, then $d = ud'$ for some unit u in R.*

Ignore "side divisors" in this course.

Exercise 22.8 (8.1/6 = Chicken McNugget Theorem)**.** Let a, b be relatively prime integers. Prove that the largest integer N for which $\nexists m, n \in \mathbb{N} : am + bn = N$ is $N = ab - a - b$.

Proof. Hi. □

23 0410

23.1 Reminders

- Final exam on Friday, May 11 from 7-10 PM in 101 LS Building.
- See RC #21 for note about 7.4 # 33 on HW # 9.
- See handout with corrected ring definitions.
- Project outlines due Thursday, in class.

23.2 Corrections to the Mods

- In the fourth bullet point, omit the sentence which reads "{0}...", and cross out the word "nontrivial".
- In the fifth bullet point, a nontrivial ring R contains at least one subring, namely R.
- Add note near section 7.3, page 239: the map $\varphi : R \to S$ by $r \mapsto 0$ is NOT a ring homomorphism unless $S = \{0\}$.

In an integral domain, the condition $\varphi(1) = 1$ can be deduced since there is a cancellation law.

23.3 Principal Ideal Domains

Euclidean domains allowed us to write GCD's as linear combinations. A more general type of ring:

$$\{\text{Euclidean domains}\} \subseteq \{\text{PID}\}$$

Definition 23.1. A *principal ideal domain*, abbreviated PID, is an integral domain in which every ideal is principal.

There are PID's which are not Euclidean domains, e.g. $\mathbb{Z}[\frac{1-\sqrt{2011}}{2}]$. In a PID, GCD's always exist, but there is no easy way to find them. Informally, "in PIDs, we still have gcds, we just don't have an algorithm to compute them."

Proposition 23.2. *(i) Suppose the ideal (a, b) can be written as (p). Then p is the GCD of a and b.*

(ii) p is an R-linear combination of a and b; that is, $\exists x, y \in R : p = xa + yb$.

(Remember: p is a gcd if $p|a$, $p|b$ and $p'|a, b \Rightarrow p'|p$. p is unique up to multiplication by a unit of R.)

Note 23.3. Let R be a commutative ring. An ideal M is maximal iff R/M is a field. An ideal P is maximal iff R/P is an integral domain. As a corollary, all maximal ideals are prime.

Hint: for final day, find a prime ideal which is not maximal.

Proposition 23.4. *In R is a PID, then every nonzero prime ideal is maximal.*

Proof. Let P be a nonzero prime ideal of a PID R. Since R is a PID, we can write it in the form $P = (p)$, where $p \in R$. We want to show that P is maximal; i.e. $\forall \text{ideal } I : P \subseteq I \subseteq R : I \in \{P, R\}$.

Let I be such an ideal. Also, let $I = (m)$, where $(p) \subseteq (m)$. Since $p \in (m)$, we have $p = mr$ for some $r \in R$. Now either $r \in P$ or $m \in P$. If $m \in P$, then it's clear that $(m) = (p)$. Otherwise, $r = sp$ for some $s \in R$. In that event, $r = smr$. since this is an integral domain, we may cancel to find that $1 = sm$; so m is a unit and thus $I = (m) = R$. □

Corollary 23.5. *If R is commutative, and the polynomial ring $R[x]$ is a PID, then R is a field.*

Proof. Consider the ideal (x). Clearly $R/(x) \cong R$. If (x) is maximal, then R would be a field. We claim that (x) is prime. So it's enough to show that R is an integral domain, but $R \subseteq R[x]$ which is an integral domain. □

Note 23.6. Check that if R is a field, $R[x]$ is in fact a Euclidean domain, by using the standard polynomial long division.

23.4 Exercises

Exercise 23.7 (8.2/1)**.** Let R be a PID. Prove that $(a) + (b) = R$ iff 1 is a gcd of a and b, where $I + J$ denotes the set $\{i + j \mid i \in I, j \in J\}$.

Proof. Check that

$$\begin{aligned} & 1 = \gcd(a, b) \\ \Leftrightarrow & \exists r, s : 1 = ra + sb \\ \Leftrightarrow & 1 \in (a) + (b) \\ \Leftrightarrow & R = (a) + (b) \end{aligned}$$

□

Exercise 23.8. 8.2/2 Let R be a PID. Prove that any two nonzero elements $a, b \in R$ have a least common multiple; i.e. an element $m \in R$ such that $a|m$, $b|m$ and $\forall m' : a|m', b|m' : m|m'$.

Proof. Let the ideal $(a) \cap (b)$ be denoted by (ℓ); this is permissible since this is a PID. We claim that ℓ is an LCM. It's clear that ℓ is a common multiple. Now $(a) \cap (b) = \{r \mid a|r, b|r\} = (\ell) = \{r \mid \ell|r\}$. Evidently if $a|\ell'$ and $b|\ell'$, we find that $\ell' \in (\ell)$ so that $\ell|\ell'$, so we're done. □

24 0412

24.1 Reminders

Final Exam: Friday May 11, 101 LS, 7-10 PM

Next project deadline: Thurs Apr 26 (check!)

24.2 Primes, Irreducibles, and Associates

Euclidean Domains are subsets of PIDs, which are subsets of UFDs.

Definition 24.1. Let R be an integral domain.

(1) An irreducible element (not zero, and not a unit) is *irreducible in* R if $r = ab \Rightarrow a$ or b is a unit in R. Otherwise, r is *reducible*.

(2) An element $p \in R$ is *prime* if it generates a prime ideal $(p) \neq R$; i.e. if $p|ab$, then either $p|a$ or $p|b$.

(3) Two nonzero elements $a, b \in R$ are *associates* if $a = bu$.

Note 24.2. Pay attention to which ring R one is working in. For example, 2 is irreducible in $R = \mathbb{Z}$ but not in $R = \mathbb{Q}$.

Proposition 24.3. *In an integral domain R, primes are irreducible.*

Proof. Suppose p is prime. Then $p \in (p)$, a prime ideal. Suppose $p = ab$ for some $a, b \in R$. Evidently one of $a, b \in (p)$; without loss of generality, $a \in (p)$. Then $a = ps$ for some $s \in R$. Now $p = psb \Rightarrow 1 = sb$, so b is a unit (since p is nonzero), and p is thus irreducible. □

The converse is *not* true in general; for example, see $\mathbb{Z}[\sqrt{-5}]$. However, we have a partial converse

Proposition 24.4. *If R is a PID, then irreducibles are prime.*

Proposition 24.5. *If R is a UFD, then irreducibles are prime.*

Proof. We'll prove the case where R is a PID; the second proposition is harder. Suppose R is a PID.

Take some irreducible element $r \in R$. In fact, we can show that (r) is a maximal ideal; this will imply that (r) is prime. Let $M = (m)$ (valid in PID) be any ideal between (r) and R. Since $r \in (r) \subseteq (m)$, we have that $r = ms$ for some $s \in R$. Since r is irreducible, either m is a unit, implying $M = R$, or s is a unit, implying $(r) = (m)$. Hence, we're done. □

24.3 UFD's

Definition 24.6. An integral domain R is a *Unique Factorization Domain* if for every non-unit $r \in R$ with $r \neq 0$, we have

(i) $r = p_1 p_2 \cdots p_n$, a finite product of irreducibles $p_i \in R$, and

(ii) This decomposition is unique up to association and re-ordering.

24.3.1 Examples of UFD's

1. $\mathbb{Z}$.
2. Fields.
3. $F[x]$ for F a field. Polynomial of x with coeffs in F.
4. $R[\{x_i\}_{i=1}^n]$ for R a UFD. Essentially multivariate polynomials in any UFD R.

24.3.2 Computing GCD's in UFD's

Suppose $r, s \in R$ and you want the gcd of r and s.

Example 24.7. Find a gcd of 120 and 48 in $\mathbb{Z}$.

Solution. I'm sure we all know how to do this. $2^3 \cdot 3 = 24$. □

Proposition 24.8. *For $r, s \in R$, let*

$$r = u \prod p_i^{\alpha_i} \quad \textit{and} \quad s = v \prod p_i^{\beta i}$$

Where u, v are units, p_i are primes, and $\alpha_i, \beta_i \in \mathbb{N}$. Then

$$(r, s) = \prod p_i^{\min(\alpha_i, \beta_i)}$$

Corollary 24.9 (FTA)**.** *$\mathbb{Z}$ is a UFD.*

Theorem 24.10. *PID's are UFD's*

Proof. Involves the Axiom of Choice. □

24.4 Polynomial Rings

Definition 24.11. let R be an integral domain and consider the ring $R[x]$. The *degree* of $f \in R[x]$. is the largest i for which the coefficient of x^i is not zero.

Proposition 24.12. *Let R be an integral domain and consider the ring $R[x]$.*

(i) $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

(ii) The units of $R[x]$ are precisely the units of R.

(iii) $R[x]$ is an integral domain.

Suppose I is an ideal of a commutative ring R. Let (I) be the ideal $I[x]$ in $R[x]$.

Fact 24.13.

$$R[x]/(I) \cong (R/I)[x]$$

In particular, if I is a prime ideal in R, then (I) is prime in $R[x]$.

Proof. We want to construct a homomorphism $R[x] \to (R/I)[x]$. It will suffice to show that φ is surjective and $\ker \varphi = (I)$. Map by

$$\sum_{i=0}^{N} r_i x^i \to \sum (r_i \mod I) x^i$$

It's clear that this is surjective, and the kernel is precisely $I[x] = (I)$.

By the First Isomorphism Theorem, we're done.

For the last remark, note that if I is prime, then R/I is an integral domain; hence $(R/I)[x]$ is an integral domain, implying thtat (I) is an integral domain. □

Note: Not all ideals of $R[x]$ are of this form.

24.5 Exercises

Exercise 24.14 (9.1/4)**.** Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal ideal.

Solution. The ideals prime since $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$ and $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$. The former is a integral domain, while the latter is a field. The conclusion follows immediately. □

Notice that this implies that $\mathbb{Q}[x, y]$ is not a PID, since prime ideals are maximal in PID's.

25 0417

25.1 Housekeeping

- Final exam: Friday May 11
  7-10 PM
  101 LSA Building
- Project rough drafts due Thursday April 26 (only nine days!!)
- Schedule project presentations ASAP.

25.2 Review

25.2.1 Chapter 8

$$\text{Fields} \subset \text{Euclidean domain} \subset PID \subset \text{UFD} \subset \text{Integral domain}$$

25.2.2 Polynomial Rings of a field

When F is a field, then the degree of a polynomial gives a norm which yields a Euclidean algorithm.

Theorem 25.1. *If F is a field, then $F[x]$ is a Euclidean domain. In particular, $F[x]$ is consequently both a UFD and PID.*

25.2.3 Examples

- $\mathbb{Q}[x]$
- $\mathbb{Z}/p\mathbb{Z}[x]$.
- $\mathbb{Q}[x, y]$ is not a PID.

The last follows because $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$. Since $\mathbb{Q}[y]$ is an integral domain, (x) is prime. On the other hand, since $\mathbb{Q}[y]$ is not a field, so (x) is prime, but not maximal.

Remember: Maximal ideals are prime, but only in PID's is the converse true.

On the other hand, $\mathbb{Q}[x, y]$ is indeed a UFD.

25.2.4 Finals: Don't Panic

- Anything is fair game on true/false and give an example. Darn.
- The final exam will be "completely fair and reasonable".
- A list of about ten proof-based questions will be given, of which two or three will appear on the final exam.
- A list of "big" theorems will be given. For some of these theorems, you will be told that you need not know the proofs.

For the rest of today, know the statements of the theorems, although you don't need the proofs.

25.3 UFD and Polynomial Rings

Theorem 25.2. *R is a UFD if and only if $R[x]$ is a UFD.*

Corollary 25.3. *If R is a UFD, then $R[x_1, \cdots, x_n]$ is a UFD for each $n \in \mathbb{Z}^+$.*

Note 25.4. Remember that $R[x_1, x_2, \cdots, x_n] \cong R[x_1, \cdots, x_{n-1}][x_n]$.

25.4 Rings of Fractions

Let R be a commutative ring, and D be a nonempty subset of $R \setminus \{0\}$ which is multiplicatively closed and contains no zero divisors.

Then there exists a commutative ring Q such that

- R is a subring of Q.
- Each element of D is a unit of Q.
- Every element of the ring of fractions Q can be written in the form $\{d^{-1}r \mid d \in D, r \in R\}$. (Remember that d^{-1} may not exist in R!.)
- Q is called a *ring of fractions* in R.
- When R is an integral domain and $D = R \setminus \{0\}$, then Q is the *field of fractions* on R.

Example 25.5. Some examples of rings of fractions.

- Let $R = \mathbb{Z}$ and $D = \mathbb{Z}^+$. In this case $Q = \mathbb{Q}$...
- Let $R = \mathbb{Z}$ and $D = \mathbb{Z} \setminus \{0\}$. Then $Q = \mathbb{Q}$, a field of fractions.
- Let $R = \mathbb{Z}$ and $D = \{2^k \mid k \in \mathbb{Z}^+\}$. Then $Q = \{\frac{n}{2^k} \mid n, k \in \mathbb{Z}, k \geq 0\} \subset \mathbb{Q}$. However, this Q here is not a field. We can also write $\mathbb{Q} = \mathbb{Z}\left[\frac{1}{2}\right]$.

Notice that we don't need $1 \in D$; since $r = d^{-1}(dr)$ the condition that $1 \in D$ isn't strictly necessary. On the other hand this is frequently the case.

In fact, for an integral domain R, taking one element from each equivalence class of associates would suffice for $D^{-1}R = Q$ to be a field. No smaller set can generate a field.

Example 25.6. When $R = F$ is a field, and D is anything nonempty, the field of fractions is simply F.

Example 25.7. Pick $R = \mathbb{Z}[x]$, and $D = R \setminus \{0\}$. Then the fraction field becomes the set of rational functions in x.

25.5 Chinese Remainder Theorem

Mm good memories.

Definition 25.8. The *direct product* of two rings R and S is the set of ordered pairs $\{(r, s) \mid r \in R, s \in S\}$, where addition and multiplication are done component-wise.

Definition 25.9. Two ideals I and J in a ring R are called comaximal if $I + J = R$.

As a special case, if I is maximal, and $J \cap I \neq I$ is a second ideal, then $I + J = R$; hence I and J are comaximal.

Recall that if $I + J = R$, then $IJ = I \cap J$. The more general $IJ \subseteq I \cap J$ holds for arbitrary ideals in R.

Below, we give CRT for the special case of two factors; it is not hard to generalize to the full version.

Theorem 25.10 (CRT)**.** *Suppose R is a commutative ring with I, J as two ideals of R.*

(1) The map $R \to R/I \times R/J$ by $r \mapsto (r + I, r + J)$ is a surjective ring homomorphism with $\ker \varphi = I \cap J$.

(2) In particular, $R/(I \cap J) \cong R/I \times R/J$.

(3) In particular, when $I + J = R$, we have $IJ = I \cap J$ so that $R/(IJ) \cong R/I \times R/J$.

Example 25.11. When $R = \mathbb{Z}$ and $I = (m)$, $J = (n)$ for $(m, n) = 1$, we have $IJ = mn\mathbb{Z}$, so that

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

25.6 Exercises

Exercise 25.12 (9.2/6)**.** Describe each of the following ring structures:

(a) $\mathbb{Z}[x]/(2)$.

(b) $\mathbb{Z}[x]/(x)$.

(c) $\mathbb{Z}[x]/(x^2)$.

(d) $\mathbb{Z}[x,y]/(x^2,y^2,2)$.

In the last ring, show that $\alpha^2 = 1$ for each α in the ring.

Find the characteristics of each of these.

Solution. (a) Polynomials in xx with coefficients in $\mathbb{F}_2$.

(b) Isomorphic to $\mathbb{Z}$.

(c) Set of linear polynomials; that is, $p(x) \equiv q(x)$ if the coefficients of x^0 and x^1 are the same.

(d) $a + bx + cy + dxy$ where $a, b, c, d \in \{0, 1\}$.

The last part follows from the "magic" $(x+y)^2 \equiv x^2 + y^2$.

The characteristics of these rings are 2, 0, 0, and 2. □

26 0419

26.1 Reminders

1. FINAL EXAM
   Fri May 1, 7-10 PM
   101 LSA Building
2. Deadline extended for project rough drafts to Friday, April 27, by midnight. Email is preferred.

26.2 Fields

Proposition 26.1. *For fields (actually integral domains), the characteristic must be either a prime p or zero.*

Proof. If $15 \cdot 1_F = 0$, then $(31_F)(51_F) = 0$, etc. □

Consider $\varphi : \mathbb{Z} \to F$ by $n \mapsto n \cdot 1_F$. In that case, we have

$$\ker \varphi = \begin{cases} \{0\} & \text{if } ch(F) = 0 \\ p\mathbb{Z} & \text{if } ch(F) = p \end{cases}$$

This can be condensed to $\ker \varphi = \operatorname{ch}(F)\mathbb{Z}$.

Then we have an injection $\mathbb{Z}/\operatorname{ch}(F)\mathbb{Z} \to F$ by $n + \operatorname{ch}(F)\mathbb{Z} \mapsto n \cdot 1_F$.

This tells us that $\mathbb{Z}/\operatorname{ch}(F)\mathbb{Z}$ sits inside of F (rather, an isomorphic copy sits in F).

Then $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq F$, or $\mathbb{Z} \subseteq F$; in fact, the latter implies $\mathbb{Q} \subseteq F$, since everything is invertible. Hence, either $\mathbb{F}_p$ or $\mathbb{Q}$ is a subfield of F.

Definition 26.2. The *prime subfield* of F is the subfield of F generated by 1_F, isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$.

This is the smallest field that contains the identity.

26.3 Field Extenisons

Definition 26.3. K is a *field extension* of a field F if K is a field containing F as a subfield. This is written as K/F and is read "K over F"; this is NOT a quotient.

Galois theory studies algebraic closures using this idea. It's a beautiful subject beyond the scope of this course.

Definition 26.4. The *degree* (or index) of a field extiension K/F is the dimension of K viewed as a vector space over F.

This is not always finite!

Question: Why study field extensions?
A: Helps us study polyonmial equations in $F[x]$.

BTW, homomorphism from a field to a field must be injections.

Theorem 26.5. *Suppose $p(x) \in F[x]$ is irreducible. Then there exists a field K such that K contains a root α of $p(x)$, and K contains (an isomorphic copy of) F.*

Proof. Take $K = F[x]/(p(x))$, the quotient by an ideal. Since $p(x)$ is irreducible, we see that $(p(x))$ is maximal... I think?

Note that $\bar{x}$ is a root of $p(x)$. Also, the constant terms alsways survive modding out, it is trivial to see that $F \subseteq K$ since $\deg p(x) \geq 1$ □

Question. How does this relate to vector spaces?

Theorem 26.6. *If $p(x) \in F[x]$ is irreducible of degree n, and $K = F[x]/(p(x))$, then $1, \bar{x}, \bar{x}^2, \cdots, \bar{x}^{n-1}$ is a basis of K over F.*

Proof. Every coset of $p(x)$ has a unique representative element of dgree at most $n-1$, implying that we can write everything as a linear combination of these terms. Linear independence also follows easily.

In other words, elements of K look like $\sum_{i=0}^{n-1} a_i \bar{x}^i$, and we can think of these as vectors. □

We also know that K is a field. Addition behaves exactly as we expect, and multiplication is... unwieldy; it is almost normal polynomial multiplication, since we are modding about $p(x)$. We can also do division by nonzero polynomials via Bezout's Lemma (cf. the reading check.)

Now, take K/F, and consider $\alpha_1, \alpha_2, \cdots \in K$. The smallest field F containing all α_i is denoted $F(\alpha_1, \alpha_2, \cdots) \subseteq K$.

Definition 26.7. Consider $F(\alpha)$. α is called a *primitive element* and the extensions are called *simple extensions.*

Theorem 26.8. *Suppose α is a root of an irreducible $p(x) \in F[x]$. Then*

$$K = F[x]/(p(x)) \cong F(\alpha)$$

26.4 Exercises

Exercise 26.9 (13.1/1)**.** Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}[\theta]$.

Solution. By Eisenstein, it's irreducible. We could also just compute with the Rational Root Theorem.

Suppose that $(1+x)(ax^2+bx+c) = 1$ in the quotient field. Then we get $1 = ax^3+bx^2+ax^2+cx+bx+c$. Then we find that

$$1 = ax^3 + (b+a)x^2 + (c+b)x + c - (ax^3 - 9ax - 6a) \tag{1}$$
$$1 = (a+b)x^2 + (b+c-9a)x + (c-6a) \tag{2}$$

So we get the system

$$a + b = 0 \tag{3}$$
$$b + c - 9a = 0 \tag{4}$$
$$c - 6a = 1 \tag{5}$$

Subtracting, we get $b - 3a = -1$; since $a + b = 0$, we can get $b = -\frac{1}{4}$. Hence $a = \frac{1}{4}$, and finally, $c = \frac{5}{2}$. □

Exercise 26.10. Let $p(x) \in \mathbb{Z}[x]$ have $p(\alpha) = 0$ for some $\alpha \in \mathbb{Q}$. Prove that α is an integer.

Solution. Rational root theorem!

Okay fine. go through the proof of the rational root theorem in the special case that the leading coefficient being 1. We're done. □

27 0424

2012 USAMO, Day 1.

28 0426

28.1 Housekeeping

Last day of actual content!

- 3 Handouts
  - Do self-evaluation now.
  - Only need project feedback if doing a project.
  - schedule for rest of semester.
- On Homework 10
  - Green percentage = HW percent so far, with two drops.
  - Red number = reading checks counted (add 1 for RC25)
- Extra Credit!

- The task is as follows... on the bspace:
  - Post a "give an example" problem. (New thread).
  - First response: give one answer.
  - Convince someone else to post another answer.
- Repeat up to 3 times (total 15 pts).
- One of the three can be "no .example exists"; then no second answer required.

28.2 Splitting Fields

28.2.1 Definition

Definition 28.1. Suppose K/F is an extension of a field F, with $f(x) \in F[x]$. Then K is a *splitting field* of $f(x)$ (over F) if $f(x)$ factors in to all linear factors in $K[x]$, and K is the smallest such field (in the sense that no proper subset of K has that property).

Example 28.2. Some examples of splitting fields...

1. Let $K = \mathbb{C}$ and $F = \mathbb{R}$. Then K is the splitting field of $x^2 + 1 \in \mathbb{R}[x]$.
2. $\mathbb{Q}(i)$ is the splitting field of $x^2 + 1$ in $\mathbb{Q}$.
3. What is the splitting field of $(x^2 - 2)(x^3 + 1) \in \mathbb{Q}[x]$? We need to have $\sqrt{2}$ as well as $\frac{1}{2}(1 + \sqrt{-3})$ and -1. it's clear then the splitting field is $\mathbb{Q}[\sqrt{2}, \sqrt{-3}]$.

Now we can get posets of inclusions. For instance,

Blah diagram.

In the last example, $\mathbb{Q}[\sqrt{2}, \sqrt{-3}]$ is a degree four extenison, even though the oriinal polynomial has degree five.

28.2.2 Results

There are a few major theorems with these definitions.

Theorem 28.3. *Splitting fileds exist.*

Theorem 28.4. *The splitting field of $f(x) \in F[x]$ is unique up to isomorphism.*

Note 28.5. For this reason, we usually refer to *the* splitting field of a $f(x) \in F[x]$.

Theorem 28.6. *If $f(X)$ has degree n, then its splitting field has index at most $n!$ over F.*

28.3 Algebraic Closures

Definition 28.7. A field F is algebracially closed if all $f(x) \in F[x]$ split into linear factors in $F[x]$.

In this case, only irreducibles are linear.

THis is one reason why we never bother building something bigger than $\mathbb{C}$: it's already algebraically closed.

Definition 28.8. The (an) *algebraic closuer* of F is a field extension $\bar{F}$ which is algebraic over F, and $\bar{F}$ is algebraically closed.

Theorem 28.9. *Algebraic closures exist.*

28.4 Exercises

Exercise 28.10. Find the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

Solution. The roots are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. clearly, we need both i and $\sqrt[4]{2}$, so the degree eight splitting field $\mathbb{Q}[\sqrt[4]{2}, i]$ is necessary and sufficient, hence we're done. □

Exercise 28.11. Find the splitting field of $x^4 + 2$ over $\mathbb{R}$.

Solution. First, note that the roots of the polynomial are

$$\pm\frac{\sqrt[4]{2}}{2}\left(\sqrt{2} \pm i\sqrt{2}\right).$$

Letting α be the above with both positive signs, the polynomial splits as

$$x^4 - 2 = (x - \alpha)(x + \alpha)(x - \bar{\alpha})(x + \bar{\alpha})$$

Clearly, $\mathbb{Q}[\sqrt[4]{2}, i]$ suffices. This is a degree-eight extension.

Let K be the splitting field. Clearly, $i\sqrt{2} \in K$; this is of degree two.

Now bash. □