MATH 356 Lecture Notes

Taught by Dr. Gregory Chambers

Shaquille Que

Spring 2020

These are my notes for Rice University's MATH 356: Abstract Algebra I, taught by Dr. Gregory Chambers. This file was created in LaTeXand uses Evan Chen's `evan.sty` package. Any mistake herein is my own. Please let me know of any errors by emailing me at stq1@rice.edu.

Contents

§1 January 14, 2020

§1.1 Group

§1.1.1 Definition

A **group** $(G, \cdot)$ is a pair composed of a nonempty set G and a binary operation, denoted by $\cdot$, on G. The operation $\cdot$ is a function $G \times G \to G$ that satisfies the following properties.

1. **associativity**. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. **existence of identity**. $\exists\, e \in G$ so that $e \cdot a = a \cdot e = a$ for all $a \in G$.
3. **existence of inverse**. $\forall a \in G$, $\exists\, b \in G$ so that $a \cdot b = b \cdot a = e$.

We denote $b = a^{-1}$.

Theorem 1.1 (Uniqueness of Identity)
The identity element e is unique.

Proof. We have $e \cdot a = a \cdot e = a$ for all $a \in G$ and $e' \cdot a = a \cdot e' = a$ for all $a \in G$. Since $e \in G$, we have $e' \cdot e = e \cdot e' = e$. Since $e' \in G$, we also have $e \cdot e' = e' \cdot e = e'$. Then $e - e \cdot e' = e'$. □

Proposition 1.2 (Uniqueness of Inverses)
The inverse of $a \in G$ is unique.

Proof. Let $a \in G$ be given and let $b, b' \in G$ be inverses of $a \in G$. By definition, we have that $a \cdot b' = e$ and $b \cdot a = e$. Then by associativity, we have that

$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'.$$

It follows that $b = b'$, so the inverse of a is unique, as desired. □

§1.1.2 Examples

- $(\mathbb{R}, +)$
  1. $+$ is a binary operation.
  2. associativity. $(a + b) + c = (a + b) + c$ holds for all $a, b, c \in \mathbb{R}$.
  3. identity. $e = 0 \implies a + 0 = a = 0 + a$ holds for all $a \in \mathbb{R}$.
  4. inverses. For $a \in \mathbb{R}$, $b = -a \implies a + b = 0 = b + a$.
- $(\mathbb{R} \setminus \{0\}, \times)$
  1. $\times$ is a binary operation.
  2. associative. $a \times b = b \times a$ for all $a, b \in \mathbb{R} \setminus \{0\}$.
  3. identity. Take $e = 1$.
  4. inverses. $a^{-1} = \dfrac{1}{a}$

- The **symmetric group** $(S_n, \circ)$, where $S_n = \{\text{all bijections from } \{1, \dots, n\}\}$ has $n!$ elements and $f \circ g$ is defined as $f(g(a))$, i.e. the composition operation.

Remark 1.3. It is possible for a binary operation to be associative but not commutative. The typical example is matrix multiplication.

Remark 1.4. As another example that commutativity $\neq$ associativity, consider the operation $x \cdot y = xy + 1$ defined on $x, y \in \mathbb{R}$. Since $x \cdot y = xy + 1 = y \cdot x$, the operation is commutative. However, we can easily check that it is not associative.

Definition 1.5. By convention, we denote e as $\mathbf{1}$ or 1_G.

Definition 1.6. By convention, we drop the $\cdot$ operation, denoting $a \cdot b$ as ab.

Definition 1.7. We may sometimes denote a group by only its set, e.g. G.

§2 January 16, 2019

Lemma 2.1

Let G be a group and $a_1, \dots, a_n$ be elements of G. For every $i \in \{1, \dots, n-1\}$,

$$(a_1 \dots a_i)(a_{i+1} \dots a_n) = a_1 \dots a_n.$$

Proof. Trivial by induction. □

Definition 2.2. The **trivial group** G has a single element $\{0\}$, with the binary operation $\cdot : G \times G \to G$ defined with $0 \cdot 0$. G satisfies associativity, with 0 as the identity element and its own inverse.

§2.1 Subgroups

Definition 2.3. A **subgroup** H of G is a subset with the following properties:

1. **closure**. For every $a, b \in H$, $ab \in H$.
2. **identity**. $\mathbf{1} \in H$.
3. **inverse**. For every $a \in H$, $a^{-1} \in H$.

Remark 2.4. The subgroup H will have the group operation **restricted** to H, i.e. $\cdot : G \times G \to G$ produces a similar operation $\cdot_H : H \times H \to H$ by restricting the domain of $\cdot$ to H. Then the closure property ensures that the range is also in H, while the other two properties ensure that H has inverses and an identity in H.

Definition 2.5. $H \leq G$ means H is a subgroup of G. $H < G$ means that H is a strict subgroup of G, i.e. $H \neq G$.

§3 January 21, 2020

Definition 3.1. $\mathbb{Z}a \stackrel{\text{def}}{=} \{n \in \mathbb{Z} \mid n = ka, k \in \mathbb{Z}\}$.

Theorem 3.2 (Subgroups of Integers Are Multiples of A Number)

If H is a subgroup of $\mathbb{Z}^+$, then H is either the trivial group, or $H = \mathbb{Z}_a$ for some positive integer a.

Proof. It is easy to show that $\mathbb{Z}_a$ is a subgroup of $\mathbb{Z}$. We consider two cases.

Case 1: H only contains 0. Then H is trivial.

Case 2: H contains a nonzero element a. Then H contains a positive integer p, since if $a < 0$, then its inverse $-a \in H$. Let q be the smallest positive integer, which we can show exists by induction. We will show that $H = \mathbb{Z}_q$.

Suppose $n \in H$. We will show that $n \in \mathbb{Z}_q$. Note that $n = kq + r$ for some $k, r \in \mathbb{Z}$, with $r \in \{0, \ldots, q-1\}$. Then $kq \in H$, so $-kq \in H$, so $n + (-kq) = n - kq \in H$, which implies that $r \in H$. But q is the smallest positive integer in H, with $r < q$, so $r = 0$. This concludes the proof. □

Proposition 3.3

Let $H = \mathbb{Z}_a + \mathbb{Z}_b$. Then $H = \mathbb{Z}_d$ is a subgroup of $\mathbb{Z}$, where $d = gcd(a, b)$.

Proof. We first show that H is a subgroup of $\mathbb{Z}$. Let $n \in H$. Then $n = ra + sb$. From this, we can easily establish that H is closed, has an identity, and has inverses, so it must be a subgroup of $\mathbb{Z}$.

□

Theorem 3.4

Let a, b be integers. Then $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_d$, where d has the following properties:

(a) d divides a and b

(b) if $e \mid a, b$, then $e \mid d$

(c) there are integers r and s such that $d = ra + sb$.

Proof. (c) is a result of the definition of $\mathbb{Z}_a + \mathbb{Z}_b$. $d \in \mathbb{Z}_d$, which means that $ra + sb = d$ for some $r, s \in \mathbb{Z}$.

(a) $a = 1a + 0b$ and $b = 0a + 1b$ both in $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_d$. Thus, $d \mid a, b$.

(b) if $e \mid a, b$, then $e \mid ra + sb$ for any r, s. Thus, $e \mid d$. □

Definition 3.5. Integers a, b are **relatively prime** if $gcd(a, b) = 1$.

Lemma 3.6 (Bezout's Identity)

a and b are relatively prime if and only if there are integers r and s such that $ra + sb = 1$.

Proof. Suppose a and b are relatively prime. Then $ra + sb = 1$ for some r, s. We also have that $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_{gcd(a,b)}$, so $1 = ra + sb$ for some r, s.

Conversely, suppose that $ra + sb = 1$. Then $gcd(a, b) = 1$¿ We have that $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_{gcd(a,b)}$. Since $ra + sb = 1$, $1 \in \mathbb{Z}_a + \mathbb{Z}_b$, so $1 \in \mathbb{Z}_{gcd(a,b)}$, so $gcd(a, b) = 1$. □

Lemma 3.7 (Prime Divisor of Product)
If p is prime and divides ab, then p divides a or p divides b.

Proof. Suppose that p does not divide a. Then $gcd(a, p) = 1$. So $1 = ra + sp$ for some r and s, so $b = rab + spb$. Since $p \mid rab, spb$, we must have $p \mid b$, as desired. □

§4 January 23, 2020

Proposition 4.1 (Intersection of Subgroups Is A Subgroup)
Let H_1 and H_2 be subgroups of G. Then $H_1 \cap H_2$ is a subgroup of G.

Proof. Let $a, b \in H_1 \cap H_2$. Then $a, b \in H_1, H_2$, so $ab \in H_1, H_2$ so $ab \in H_1 \cap H_2$, so $H_1 \cap H_2$ is closed.

e_G must be in both H_1, H_2, so $H_1 \cap H_2$ contains an identity element. Proving inverses follows similarly. □

Lemma 4.2 (Properties of LCM)
Let $a, b \neq 0$ and $\mathbb{Z}_c = \mathbb{Z}_a \cap \mathbb{Z}_b$. Then $c = \text{lcm}(a, b)$

1. $a \mid c$ and $b \mid c$
2. for every $m \in \mathbb{Z}$ such that $a \mid m$ and $b \mid m$, then $c \mid m$.

Proof. For 1, we have that $c \in \mathbb{Z}_a \cap \mathbb{Z}_b$, so $c \in \mathbb{Z}_a$ and $c \in \mathbb{Z}_b$. It follows that $a, b \mid c$.

For 2, we know that $m \in \mathbb{Z}_a \cap \mathbb{Z}_b$, so $m \in \mathbb{Z}_c$ implies that $c \mid m$. □

§4.1 Cyclic Subgroups

§4.1.1 Motivation

Let G be a group with $x \in G$. What happens to all the powers of x in G? Let $X = \{x^k \mid k \in \mathbb{Z}\}$. It turns out that X is a subgroup of G.

But do all of the elements need to be distinct? It turns out the answer is no. The simplest counterexample is the trivial group.

Proposition 4.3 (Existence of Orders)
If $\{x^k\}$ are not all distinct in G, then there is some $n \geq 1$ such that

$$\{x^k \mid k \in \mathbb{Z}\} = \{x^0, x^1, \ldots, x^{n-1}\}.$$

Proof. Let $S \subseteq \mathbb{Z}$ be all the powers k so that $x^k = 1$. Then S cannot be empty, since $x^i = x^j$ with $i < j$ implies that $1 = x^{j-i}$, so S contains a positive integer. We show that S is a subgroup of $\mathbb{Z}^+$.

If $k, \ell \in S$, then $x^k = x^\ell = 1$, so that $x^{k+\ell} = 1$, which shows that S is closed under addition. We also have that $x^0 = 1$ is an identity for S, and $x^{-k} = 1$ is the inverse of x^k. It follows that S is a subgroup of $\mathbb{Z}^+$, which implies that $S = \mathbb{Z}_c$ for some c.

For every $m \in \mathbb{Z}$, let $m = zc + r$, for some $z \in \mathbb{Z}$ and $r \in \{0, \ldots, c-1\}$. Then $x^m = x^{zc+r} = (x^c)^z x^r = x^r$. Thus, we have that $\{x^m \mid m \in \mathbb{Z}\} = \{x^0, \ldots, x^{c-1}\}$. These elements are all distinct, since if there were $0 \leq i < j \leq c-1$ with $x^i = x^j$, then $x^{j-i} = 1$, with $j - i < c$. This contradicts the minimality of c. □

Definition 4.4. n is the **order** of x.

Proposition 4.5 (Lagrange)
If G is a finite group with $|G| = m$, then $x^n = 1, x^m = 1$ and $n \mid m$.

§4.2 Homomorphism

Definition 4.6. Let G and G' be groups. A function $\phi : G \to G'$ is a **homomorphism** if for every a and b in G,

$$\phi(a \cdot_G b) = \phi(a) \cdot_{G'} \phi(b)$$

or equivalently, $\phi(ab) = \phi(a)\phi(b)$.

Example 4.7 (Trivial Homomorphism)
The **trivial homomorphism** with $\phi : G \to G'$ and $\phi(a) = 1_{G'}$.

Example 4.8 (Inclusion Homomorphism)
Let H be a subgroup of G. Then $\phi : H \to G$ with $\phi(a) = a$ is the **inclusion homomorphism**.

Example 4.9 (Exponential Function)
$\phi : \mathbb{R}^+ \to \mathbb{R}^\times$ with $\phi(x) \stackrel{\text{def}}{=} e^x$.

§4.2.1 Properties

Homomorphisms preserve the following group structures:

1. $\phi(1_G) = 1_{G'}$.

   Proof. $\phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G) \implies \phi(1_G) = 1_{G'}$. □

2. $\phi(a^{-1}) = \phi(a)^{-1}$.

   Proof. $1_{G'} = \phi(1_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. □

Remark 4.10. This is similar to linear transformations in linear algebra.

§5 January 28, 2020

Definition 5.1. The **image** of ϕ is defined by $\text{im}(\phi) = \{g \in G' \mid \exists\, a \in G, \phi(a) = g\}$.

Definition 5.2. The **kernel** of ϕ is defined by $\ker(\phi) = \{g \in G \mid \phi(g) = 1_G\}$.

Proposition 5.3 (Image and Kernel Are Subgroups)
$\text{im}(\phi)$ and $\ker(\phi)$ are subgroups of G'.

Proof. Let $a, b \in \text{im}(\phi)$. Then $a = \phi(g), b = \phi(h)$ where $g, h \in G$. It follows that $ab = \phi(g)\phi(h) = \phi(gh) \in G'$. Let $a \in \text{im}(\phi)$. Then $a = \phi(g), g \in G$. Let $b = \phi(g^{-1}) = \phi(g)^{-1}$, so $ab = ba = 1_G$. Finally, $\phi(1_G) = 1_{G'}$.

Let K be the kernel of ϕ. If $a, b \in K$, then $ab \in K$, implying $\phi(ab) = \phi(a)\phi(b) = 1_{G'}1_{G'} = 1_{G'}$. Note that $\phi(a) = 1_{G'}$, so $\phi(a^{-1}) = \phi(a)^{-1} = (1_{G'})^{-1} = 1_{G'}$. Finally, $\phi(1_G) = 1_{G'}$, as desired. □

§5.1 Cosets

Definition 5.4. Let H be a subgroup of G, and let $a \in G$. The **left coset** of H with respect to a is given by $aH = \{ah \mid h \in H\}$. Similarly, the **right coset** of H with respect to a is given by $Ha = \{ha \mid h \in H\}$.

Lemma 5.5 (Coset Properties of the Kernel)
Let $\phi : G \to G'$ be a homomorphism, $K = \ker(\phi)$, and $a, b \in G$. The following are equivalent:

1. $\phi(a) = \phi(b)$
2. $a^{-1}b \in K$
3. b is an element of aK
4. $aK = bK$.

Proof. 1 $\implies$ 2: We have that $\phi(a) = \phi(b)$ implies that $\phi(a)^{-1}\phi(b) = 1$, which implies that $\phi(a^{-1}b) = 1$, as desired.

2 $\implies$ 1: $\phi(a^{-1}b) = 1$ implies that $\phi(a^{-1}) = \phi(b) = 1$, so $\phi(a)^{-1}\phi(b) = 1$, yielding $\phi(b) = \phi(a)$, as desired.

2 $\implies$ 3: Let $a^{-1}b = k$, with $k \in K$. Then $b = ak \in aK$, as desired.

3 $\implies$ 2: $b = ak$, $k \in K$ implies that $a^{-1}b = k$, so $a^{-1}b \in K$.

3 $\implies$ 4: $b \in aK \implies b = a\tilde{k}$ for some $\tilde{k} \in K$. Then $a = b\tilde{k}^{-1}$, and $ak_1 = b\tilde{k}^{-1}k_1$ for any $k_1 \in K$. Since $k^{-1}k_1 \in K$, it follows that $aK \subseteq bK$. Similarly, we have that $bk_2 = (a\tilde{k})k_2 \in aK$, so $bK \subseteq aK$.

4 $\implies$ 3: $b \in bK = aK$. □

Lemma 5.6 (Injectivity Means Kernel Is Trivial)
ϕ is injective if and only if $\ker(\phi) = \{1_{G'}\}$.

Proof. Suppose ϕ is injective. Let $a \in K$. We have that $1_G \in K$, so $\phi(a) = \phi(1_G)$ implies that $a = 1_G$, as desired.

If K is trivial, and $\phi(a) = \phi(b)$ for $a, b \in G$, then $a^{-1}b \in K$ by Lemma 5.5, so $a^{-1}b = 1 \implies a = b$, as desired. □

Definition 5.7. Let $a, g \in G$. Then gag^{-1} is the **conjugate** of a by g.

Definition 5.8. A subgroup N of G is **normal** if for every $a \in N$, $g \in G$, $gag^{-1} \in N$.

Lemma 5.9 (Kernels Are Normal)
Let $\phi : G \to G'$ be a homomorphism. Then $\ker(\phi)$ is a normal subgroup of G.

Proof. Let $a \in K$, $g \in G$. We want to show that $gag^{-1} \in K$. We have that $\phi(a) = 1_{G'}$, so $\phi(gag^{-1}) = \phi(g)1_{G'}\phi(g)^{-1} = 1_{G'}$, as desired. □

Definition 5.10. The **center** of G is the set of all elements that commute with everything.

$$Z = \{z \in G \mid xz = zx \quad \forall x \in G\}.$$

Remark 5.11. Z is non-empty, since $1_G \in Z$.

Remark 5.12. Z is a normal subgroup, since $gzg^{-1} = gg^{-1}z = z \in Z$.

§5.2 Isomorphisms

Definition 5.13. $\phi : G \to G'$ is an **isomorphism** if ϕ is a homomorphism and is bijective. We denote this by $G \cong G'$.

Remark 5.14. An isomorphism preserves group structure.

Remark 5.15. Since ϕ is bijective, we can define the inverse function of ϕ by $\phi^{-1} : G' \to G$, which is also a homomorphism.

Lemma 5.16 (Inverse of Isomorphism Is An Isomorphism)
ϕ^{-1} is also an isomorphism.

Inverse of Isomorphism Is An Isomorphism. It is easy to show that ϕ^{-1} exists and is a bijection. For $x, y \in G$, we have that $\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy = \phi(\phi^{-1}(xy))$, and since ϕ is injective, $\phi^{-1}(x)\phi^{-1}(y) = \phi^{-1}(xy)$, as desired. □

Idea

Let $H \leq G$. We look at the collection of all $[aH]$ and all $[Ha]$ and show that either a_1H and a_2H are either the same or are disjoint.

$|aH| = |H| \mid |G|$.

§6 January 30, 2020

§6.1 Equivalence Relations and Partitions

Let S be a set.

Definition 6.1. A **relation** on S, denoted by R is a subset of $S \times S$. We use the notation $x \sim y$ to mean that $(x, y) \in R$.

Definition 6.2. A relation R is an **equivalence relation** if it satisfies the following three properties:

1. **transitivity**. $x \sim y$ and $y \sim z$ implies $x \sim z$ for $x, y, z \in S$.
2. **reflexivity**. $s \sim x$ for all $x \in S$.
3. **symmetry**. $x \sim y$ implies $y \sim x$.

Example 6.3 (Relations Defined By Functions)
Let $f : A \to B$ be a function. The relation defined by $a \sim b$ if $f(a) = f(b)$ for $a, b \in A$.

Definition 6.4. $C_a \stackrel{\text{def}}{=} \{b \in S \mid a \sim b\}$ is the **equivalence class** of $a \in S$.

Example 6.5 (Circle Equivalence Class)
For $f(x, y) = \sqrt{x^2 + y^2}$ and the relation given by $a \sim b$ if $f(a) = f(b)$, C_a is the circle that contains a.

Definition 6.6. A collection of non-empty subsets Π of S is a **partition** if

1. $\bigcup_{\alpha \in \Pi} \alpha = S$
2. if $\alpha, \beta \in \Pi$, then either $\alpha = \beta$ or $\alpha \cap \beta = \emptyset$.

Proposition 6.7 (Equivalence Classes Form Partitions)
The collection of equivalence classes forms a partition of S. Conversely, if Π is a partition of S, then there exists an equivalence relation so that its equivalence classes are equal to the elements of Π.

Proof. We prove the latter statement first. Define $\sim$ by $a \sim b$, $a, b \in S$, if a and b are both elements of $\alpha \in \Pi$. This relation is transitive ($a \sim b$ and $b \sim c$ implies $a, b, c \in \alpha \in \Pi$, so $a \sim c$), reflexive ($a \sim a$ since a must be contained in some $\alpha \in \Pi$), and symmetric ($a \sim b$ implies $a, b \in \alpha \in \Pi$, so $b \sim a$), so it must be an equivalence relation.

We now prove the first statement. Each element $a \in S$ is contained in an $\alpha \in \Pi$, so $\bigcup_{\alpha \in \Pi} \alpha = S$. Now for $\alpha, \beta \in \Pi$, if $\alpha = \beta$, then we are done. Otherwise, assume $\alpha \neq \beta$ and suppose there is a $c \in C_a$ but not in C_b (without loss of generality). Let $d \in C_a$ and $f \in C_b$. Then $a \sim d$ and $b \sim f$. If $d = f$, then $a \sim c$ implies that $b \sim c$ by transitivity, a contradiction. Thus, $\alpha \cap \beta = \emptyset$. This completes the proof. □

Left Cosets

Define an equivalence relation on G with $a \sim b$ iff $a = bh$ for some $h \in H$.

1. transitivity. $a \sim b$ and $b \sim c$ implies $a = bh_1 = bh_2h_1$, where $h_2h_1 \in H$.
2. $a \sim a$ since $a = a1_G$.
3. $a \sim b$ implies $b \sim a$ since $a = bh$ implies $b = ah^{-1}$.

Then $C_a = \{b \mid a \sim b\} = \{b \mid a = bh \text{ for some } h \text{ in } H\} = \{b \mid b = ah^{-1} \text{ for some } h \text{ in } H\} = \{b \mid b = ak \text{ for some } k \text{ in } H\} = aH$.

Hence the equivalence classes are the left cosets of H, and the left cosets of H partition G.

Lemma 6.8 (Left Cosets Have Same Order As Group)
aH has the same order as H.

Proof. Define $f : H \to aH$ by $f(x) \stackrel{\text{def}}{=} ax$. Then f is a bijection, with $f^{-1}(y) = a^{-1}y$. So both are infinite, or both are finite and contain the same number of elements. □

Definition 6.9. $[G : H]$ is the number of left cosets of H in G.

Lemma 6.10 (Counting Formula)
$|G| = [G : H]\,|H|$.

Proof. This follows from the fact that all cosets have the same order, and that they partition the group. □

Theorem 6.11 (Lagrange's Theorem)
Let H be a subgroup of G. Then $|H|$ divides $|G|$.

Proof. This follows from the previous lemma. □

§7 February 4, 2020

Corollary 7.1 (Order of Element Divides Group Order)
If G is a finite group and $x \in G$, then the order of x divides the order of G.

Proof. Since $\langle x \rangle \leq G$, by Lagrange's Theorem, we must have that $|\langle x \rangle| \mid |G|$. □

Corollary 7.2 (Order of Element Of Group With Prime Order)
Let G be a finite group with prime $p = |G|$. If $x \in G$, then the order of x is either 1 or p.

Proof. If x is the identity, then $|\langle x\rangle| = 1$. Otherwise, x is not the identity, so $2 \leq |\langle x\rangle| \leq p$ with $|\langle x\rangle| \mid p$ implies that $|\langle x\rangle| = p$, as desired. □

Corollary 7.3 (Order Properties of Homomorphisms)
Let $\phi : G \to G'$ be a homomorphism, where G, G' are both finite. Then the following are true.

1. $|G| = |\ker \phi|\,|\operatorname{Im} \phi|$.
2. $|\ker \phi|$ divides $|G|$.
3. $|\operatorname{Im} \phi|$ divides $|G|$ and $\left|G'\right|$.

Proof. The first formula follows from $[G : \ker \phi] = |\operatorname{Im} \phi|$, which can be obtained by noting that the bijective function $f : \{\text{left cosets of } \ker \phi\} \to \operatorname{Im} \phi$ defined by $f(a \ker \phi) \overset{\text{def}}{=} \phi(a)$.

The second formula follows from Lagrange's theorem since $\ker \phi \leq G$, and the third formula also follows from Lagrange's. □

Proposition 7.4 (Multiplicative Property of the Index)
If $K \leq H \leq G$, then $[G : K] = [G : H][H : K]$.

Proof. Suppose $m = [G : H]$ and $n = [H : K]$ are finite. Let $G = g_1H \cup \cdots \cup g_mH$, all distinct, and $H = h_1K \cup \cdots \cup h_nK$. It is easy to show that $G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} g_ih_jK$, e.g. by noting that $g_iH = g_ih_1K \cup \cdots \cup g_ih_nK$ is a partition of the coset g_iH. Thus, G is partitioned into the mn cosets g_ih_jK, as desired. □

§7.1 Right Cosets

Remark 7.5. Right cosets also partition G.

Remark 7.6. In general, it is not true that $gH = Hg$. For example, we can consider $G = S_3$ and $H\{id, (12)\}$. Groups that have this property are normal subgroups.

§8 February 6, 2020

Proposition 8.1 (Normal Subgroups Agree On Left And Right Cosets)
Let H be a subgroup of G. The following are equivalent.

1. H is a normal subgroup.
2. For $g \in G$, $gHg^{-1} = H$.
3. For $g \in G$, $gH = Hg$.
4. Every left coset of H in G is a right coset.

Proof. (1 $\implies$ 2) Let H be normal. Since H is normal, we have $gHg^{-1} \subseteq H$. We show that $H \subseteq gHg^{-1}$. Since H is normal, take $g^{-1} \in G$. Then $g^{-1}Hg \in H$. Thus, $g^{-1}Hg \subseteq H$, so $gg^{-1}Hgg^{-1} \subseteq gHg^{-1}$ implies $H \subseteq gHg^{-1}$. Thus, $gHg^{-1} = H$.

(2 $\implies$ 1) Trivial.

(2 $\iff$ 3) We have $gHg^{-1} = H$ for all $g \in G$ iff $gH = gHg^{-1}g = Hg$ for all $g \in G$.

(3 $\implies$ 4) Trivial.

(4 $\implies$ 3) Let gH be a left coset. Then there must be a $g' \in G$ such that $gH = Hg'$. Since the right cosets of H partition G, then we must have either $Hg' = Hg$ or $Hg' \cap Hg = \emptyset$. However, we note that $g \in gH = Hg'$ and $g \in Hg$, so $Hg' \cap Hg \neq \emptyset$. Thus, we must have $gH = Hg' = Hg$, as desired.

This concludes the proof. □

Proposition 8.2 (Conjugation of Subgroup Is Still A Subgroup)
If $H \leq G$ and $g \in G$, then gHg^{-1} is a subgroup of G.

Proof. Just note that conjugation by G is an automorphism of G. □

Proposition 8.3 (Subgroups With Unique Orders Are Normal)
If $H \leq G$ and H is the only subgroup of order r, then H is normal.

Proof. Let $g \in G$. We show that $gHg^{-1} = H$. By Proposition 8.2, we have that gHg^{-1} is a subgroup of G. Let $f : H \to gHg^{-1}$ be a mapping defined by $f(x) \stackrel{\text{def}}{=} gxg^{-1}$. It is easy to see that f is a bijection. Since H is the only subgroup with r elements, $gHg^{-1} = H$, so $H \trianglelefteq G$. □

§8.1 Modular Arithmetic

Definition 8.4. $a \equiv b \pmod{n}$, $n > 0$, means that $n \mid b - a$.

Remark 8.5. We can think of this as an equivalence relation. $a \sim b$ if $n \mid b - a$.

Claim 8.6. There are n equivalence classes given by $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$.

Proof. Easy to show. □

Proposition 8.7 (Properties of Modulo Operator)
Let $n > 0$ and $a, b, a', b' \in \mathbb{Z}$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Proof. Also easy to show. □

§9 February 11, 2020

§9.1 Product Groups

Definition 9.1. Let G, G' be groups. The **product group** is the set $G \times G'$ along with the binary operation

$$(a, a') \cdot_{G \times G'} (b, b') \stackrel{\text{def}}{=} (a \cdot_G b, a' \cdot_{G'} b')$$

Proposition 9.2 (Functions on Product Group To Supergroup)

Let H and K be subgroups of G, and let $f : H \times K \to G$ be defined by $f(h,k) = hk \in G$.

1. f is injective if and only if $H \cap K = \{1\}$.
2. f is a homomorphism from $H \times K \to G$ if and only if elements of H commute with elements of K.
3. If H is a normal subgroup of G, then HK is a subgroup of G.
4. f is an isomorphism if and only if $H \cap K = \{1\}$, $HK = G$, and H, K are normal subgroups of G.

Proof. We prove each statement.

1. Suppose that $x \in H \cap K$, Then $x^{-1} \in H \cap K$ too, so $f(x^{-1}, x) = 1 = f(1,1)$. Since f is injective, then $x = 1$, as desired. Conversely, if $H \cap K = \{1\}$, then $f(h_1, k_1) = f(h_2 k_2)$ implies that $h_1 k_1 = h_2 k_2$, and so $k_1 k_2^{-1} = h_1^{-1} h_2$. Since $k_1 k_2^{-1} \in K$ and $h_1^{-1} h_2 \in H$, their equality implies that they are in $H \cap K = \{1\}$. So we get that $k_1 = k_2, h_1 = h_2$, and thus f must be injective. □
2. Let $(h_1, k_1), (h_2, k_2) \in H \times K$. Then $f((h_1, k_1) \cdot (h_2, k_2)) = f(h_1, k_1) f(h_2, k_2) \iff h_1 h_2 k_1 k_2 = f(h_1 h_2, k_1 k_2) = h_1 k_1 h_2 k_2 \iff h_2 k_1 = k_1 h_2 \iff$ every element from H commutes with every element from K. □
3. Let $H \trianglelefteq G$. Then for every $k \in K$, $kH = Hk$ by Proposition 8.1. Using this, it is easy to show that $HK = KH$. We cam also show that this is a subgroup. Note that $(HK)(HK) = HKHK = HHKK = HK$, so the set is closed under the operation. It is easy to show that HK contains inverses and the identity of G. □
4. Suppose f is an isomorphism. Then $HK = \operatorname{Im} f = G$ since f is surjective. Similarly, f is injective, so $H \cap K = \{1\}$. Let $M = H \times \{1\} \subseteq H \times K$. Then M is normal, since $(h_1, k_1) M (h_2, k_2) = \{h_1 h h_2, k_1 1 k_2 \mid h \in H\} = H \times K$. Then $f(M) = H \subseteq G$. Since $M \trianglelefteq H \times K$, $H = f(M)$ is normal in G. We can use $M = \{1\} \times K$ to show that $K \trianglelefteq G$ as well.

   Suppose now that these three properties hold. We show that f is an isomorphism. Since $HK = G$, f is surjective, and since $H \cap K = \{1\}$, then f is also injective. Thus, f is bijective. To show that f is a homomorphism, it suffices to show that for $h \in H, k \in K$, we have that $hk = kh$, or equivalently, $hkh^{-1}k^{-1} = 1$. We show that $hkh^{-1}k^{-1} \in H, K$. Since H, K are normal, then $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in Kk = K$, and $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in hH = H$, so $hkh^{-1}k^{-1} \in H \cap K$, so that it must be the identity, as desired. □

§10 February 18, 2020

Proposition 10.1 (Isomorphism Classes of Groups of Order 4)

There are two isomorphism classes of groups of order 4, the cyclic group C_4, and the Klein Four Group isomorphic to $C_2 \times C_2$.

Sketch of proof. Consider the cases when G contains an element of order 4 and when it doesn't. □

§10.1 Quotient Groups

Definition 10.2. Let $N \trianglelefteq G$. Define $\overline{G}$ to be the set of all left cosets of N in G.

Definition 10.3. Let $X, Y \in \overline{G}$. Define $X \cdot Y \stackrel{\text{def}}{=} \{xy \mid x \in X, y \in Y\}$. $XY \subseteq G$.

Claim 10.4. $XY \in \overline{G}$.

Proof. Let $X = aN, Y = bN$ for some $a, b \in G$. Then $XY = (aN)(bN) = aNNb = aNb = abN$. □

Definition 10.5. It is easy to verify that this operation has all of the properties of a group operation. Thus, $\overline{G}$ is a group, which we will denote by G/N.

Theorem 10.6 (First Isomorphism Theorem)
Let G and G' be groups and $\phi : G \to G'$ be a surjective homomorphism with $\ker \phi = K$. Then $G/K \cong G'$, and if ϕ is not surjective, then $G/K \cong \operatorname{Im} \phi$.

Does $gkg^{-1} \in K$? Yes, $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1$.

We can easily show that $f : G/K \to G'$ defined by $f(X) \stackrel{\text{def}}{=} \phi(x)$ for any $x \in X$ satisfies that f is a bijection and a homomorphism.

§11 February 20, 2020

Question 11.1. If $K \leq G \times G'$, are there always subgroups $H \leq G, L \leq G'$ so that $K = H \times L$?

The answer is no. We give the following examples.

Example 11.2
Let G be any nontrivial group and $G' = G$. Define $K = \{(g, g) \mid g \in G\}$. Then $K \subseteq G \times G$ (easy to verify), but there are no subgroups H and L of G so that $K = H \times L$.

Theorem 11.3 (Fermat's Little Theorem)
Let p be a prime number and a a positive integer. Then

$$a^p \equiv a \pmod{p}.$$

Proof. We consider the following cases.

Case 1: $a = kp$. Then $a \equiv 0 \pmod{p} \equiv a^p \pmod{p}$.

Case 2: $a \not\equiv 0 \pmod{p}$. Then $\mathbb{Z}/p\mathbb{Z}$ represents the p equivalence classes of $\mathbb{Z} \mod p$ and $\mathbb{Z}/p\mathbb{Z}^\times$ represents the $p-1$ equivalence classes (it is easy to see that 0 is not in this class). Then $|\langle \bar{a} \rangle|$ divides $p - 1 = \left|\mathbb{Z}/p\mathbb{Z}^\times\right|$ by Lagrange's Theorem. It follows that $a^{p-1} = 1$, so $a^p = a$, as desired. □

§11.1 Group Actions

Definition 11.4. A **group action** or group operation is an operation $\star$ defined on a group G and set S by $\star : G \times S \to S$ that satisfies the following.

1. *identity.* $1 \star s = s$ for every $s \in S$.
2. *associativity.* $(g_1 g_2) \star s = g_1 \star (g_2 \star s)$ for every $g_1, g_2 \in G$ and $s \in S$.

Example 11.5 (Symmetric Group Action)

Let $\sigma \in G = S_n$ and $i \in S = \{1, \ldots, n\}$. Define $\sigma \star i \stackrel{\text{def}}{=} \sigma(i) \in S$. It is easy to verify that identity and associativity holds.

Example 11.6 (Groups Are Just Sets With Group Actions)

Let $S = G$. Define $g \star s \stackrel{\text{def}}{=} gs$. Then $\star$ is equivalent to the operation of the group.

Remark 11.7. Group actions allow us to work with sets that aren't groups.

Example 11.8

The isometries of $\mathbb{R}^2$ that preserve the square $= G$.

Definition 11.9. An **isometry** of $\mathbb{R}^2$ is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $d(f(x), f(y) = d(x, y)$. The only isometries of $\mathbb{R}^2$ are

1. rotations
2. translations
3. reflections
4. glide (reflection along a line ℓ followed by a translation parallel to ℓ)

all of which are bijections. These form a group under composition.

Remark 11.10. In general, if we fix $g \in G$, we get a function $f_g : S \to S$ defined by $f_g(s) \stackrel{\text{def}}{=} g \star s$. This is a bijection, with inverse function $f_{g^{-1}}$.

§12 February 25, 2020

§12.1 Orbits

Definition 12.1. Let $s \in S$. The **orbit** of s is denoted by $\mathcal{O}_s = \{s' \in S \mid s' = g \star s \text{ for some } g \in G\}$.

Example 12.2

S_n acts on $\{1, \ldots, n\}$ by evaluation $\sigma \in S_n, i \in \{1, \ldots, n\}$, $\sigma \star i \stackrel{\text{def}}{=} \sigma(i)$.

For any $j \in \{1, \dots, n\}$, then we can find a $\sigma \in S_n$ so that $\sigma(i) = j$, $\sigma = (i, j)$, $\mathcal{O}_1 = \{1, \dots, n\} = S$.

Definition 12.3. An action is **transitive** if it only has one orbit.

Remark 12.4. Define a relation $s \sim s'$ if $s' \in \mathcal{O}_s$. This is an equivalence relation, and the equivalence class of s' is $\mathcal{O}_s$.

Proposition 12.5 (First Counting Formula)

If S is finite, then

$$|S| = \sum_{\text{distinct orbits } \mathcal{O}_s} |\mathcal{O}_s|$$

Each orbit is nonempty, and the union is S, a finite set, and so there can only be finitely many of the.

Example 12.6

Let M be the group of isometries on $\mathbb{R}^2$. Then M acts on $\mathbb{R}^2$, and for $z \in \mathbb{R}^2$, $f \in M$, $f \star z \stackrel{\text{def}}{=} f(z)$. This action is transitive.

Sketch of proof. There is a translation f by z such that $f \star (0,0) = (0,0) + z = z$. So the orbit of $(0,0)\mathcal{O}_{(0,0)} = \mathbb{R}^2$ is transitive. □

Example 12.7

M with S being the set of all triangles in $\mathbb{R}^2$.

In particular, for a triangle T whose vertices are $(0,0), (0,1), (1,0)$, and $f \in M$, then $f(T) \subseteq \mathbb{R}^2$ is a triangle. $\mathcal{O}_T$ are all the congruent triangles to T. However, the triangle $\tilde{T} = (0,0), (0,2), (2,0)$ has the property that $\tilde{T} \neq f \star T$ for any $f \in M$ since f preserves distances.

§12.2 Stabilizers

Definition 12.8. The **stabilizer** of an element $s \in S$ is the set of all $g \in G$ such that $g \star s = s$, i.e. $\text{stab}(s) = \{g \in G \mid g \star s = s\}$. Then $\text{stab}(s) \leq G$.

Proposition 12.9

If G acts on S and $H = \text{stab}(s)$ for some $s \in S$, then

1. $a, b \in G$, $a \star s = b \star s$ if and only if $a^{-1}b \in H$.
2. If $a \star s = s'$ and $H' = \text{stab}(s')$, then $H' = aHa^{-1}$.

Proof. 1. $a \star s = b \star s \iff a^{-1} \star (a \star s) = a^{-1} \star (b \star s) \iff s = (a^{-1}b) \star s \iff a^{-1}b \in H$.

2. $H' \subseteq aHa^{-1}$ and $aHa^{-1} \subseteq H'$ and $aHa^{-1} \subseteq H'$. Then $a^{-1} \star (a \star s) = s = a^{-1} \star s'$. So $(aha^{-1}) \star s' = (ah) \star (a^{-1} \star s') = (ah) \star s = a \star (h \star s) = a \star s = s'$, so $aha^{-1} \in H'$.

   Let $b = a^{-1}$, so that $s = b \star s'$. Then $bH'b^{-1} \subseteq H$ by the same proof, so $H'b^{-1} \subseteq b^{-1}H$, so $H' \subseteq b^{-1}Hb = aHa^{-1}$.

□

Remark 12.10. Elements in the same orbit have stabilizers related by conjugation.

§12.3 Actions on Cosets

For a group G and subgroup H of G, there is a natural group action of G on left cosets of H (note that H may bot be normal). G/H is the set of left cosets if H is not normal.

Definition 12.11. $LC(H)$ is the set of left cosets of H.

Definition 12.12. Let $S = LC(H)$. Then we define the group action by $g \star C \stackrel{\text{def}}{=} \{gc \mid c \in C\} \subseteq G$ for $g \in G, C \in LC(H)$.

We check that $g \star C$ is still in S, i.e. that it is a left coset of H. $g \star C = \{gc \mid c \in C\} = \{gah \mid h \in H\} = (ga)H \in LC(H)$.

We also check that this is a group action. $1 \star C = C$ and $(g_1 g_2) \star C = (g_1 g_2) \star aH = (g_1 g_2 \star a)H$.

Proposition 12.13 1. This action is transitive.

2. $\text{stab}(H) = H$.

Proof. 1. Given a left coset aH, we want to find some $g \in G$ so that $g \star H = aH$. Then just choose $g = a$.

2. $g \in \text{stab}(H) \iff g \star H = H \iff g \in H$.

□

§13 February 27, 2020

Proposition 13.1 (Second Counting Formula)

Let $s \in S$. There is a bijection between the left cosets of $H = \text{stab}(H)$ and $\mathcal{O}_s$ where $H = \text{stab}(s)$. And for every left coset C of H and $g \in G$,

$$\epsilon(gC) = g \star \epsilon(C).$$

Proof. We define ϵ by

$$\epsilon(C) \stackrel{\text{def}}{=} a \star s \in \mathcal{O}_s$$

where $C = aH$ for some $a \in G$. We show that ϵ is well defined. Let $C = aH = bH$ for some $a, b \in C$. We show that $a \star s = b \star s$. From $aH = bH$, we have that $a = bh$ for some $h \in H$, so $b^{-1}a = h$ for some $h \in H$. Since $h \in H = \text{stab}(s)$, we have $h \star s = s$, so $(b^{-1}a) \star s = s \implies b^{-1} \star (a \star s) = s \implies (b \star b^{-1}) \star a \star s = b \star s \implies (bb^{-1}) \star a \star s = b \star s \implies a \star s = b \star s$, so ϵ is well-defined.

We now show that ϵ is a bijection. Given $s' \in \mathcal{O}_s$, we have that $s' = g \star s = \epsilon(gH)$ for some $g \in G$. Thus, ϵ is surjective. To see that ϵ is also injective, suppose that

$\epsilon(C) = \epsilon(D)$ for some left cosets C and D of H. Let $C = aH$, $D = bH$ for some $a, b \in G$. Then $\epsilon(C) = a \star s \in \mathcal{O}_s$ and $\epsilon(D) = b \star s \in \mathcal{O}_s$, so $a \star s = b \star s$ implies that $(b^{-1}a) \star s = s$, which implies that $b^{-1}a \in H$. Then $a = bh$ for some $h \in H$, so $aH = bH$, as desired.

If $g \in G$, let $C \in LC(H) = G/H$. Then $C = aH$ for some $a \in G$. We have that $g \star \epsilon(C) = g \star (a \star s) = (ga) \star s = \epsilon(gC)$, so $gC = (ga)H$.

This yields the counting formula. □

Corollary 13.2

In particular, if G and S are finite, $s \in S$, $H = \text{stab}(s) \leq G$, then by Lagrange's Theorem,

$$|G| = [G : H]\,|H| = |\mathcal{O}_s|\,|\text{stab}(s)|\,.$$

Remark 13.3. Let X be the set of all subsets of G of r elements. There is a natural group action of G on X such that for $U \in X$, $U \subseteq G$, $|U| = r$, and $g \star U \overset{\text{def}}{=} \{gu \mid u \in U\}$. For any $u_1, u_2 \in U$, since g has an inverse, we have that $gu_1 = gu_2 \implies u_1 = u_2$, so $|g \star U| = r$. Then $1 \star U = U$ and $(ab) \star U = a \star (b \star U)$ since G is a group and group multiplication is associative.

Definition 13.4. A **permutation representation** of G of order n is a homomorphism $\Phi : G \to S_n$.

Note that $\Phi(g) \in S_n$ and $\Phi(g)(i) \in S = \{1, \ldots, n\}$, where $i \in S$. For example, we can take Φ to send every $g \in G$ to the identity permutation $\Phi(g)(i) = i$ for all g, i.

Proposition 13.5

There is a bijection between operations of G on $S = \{1, \ldots, n\}$ and the permutation representations $G \to S_n$.

Proof. We start with an action $\star$ of G on S and build a homomorphism from G to S_n. Call this homomorphism $\Phi : G \to S_n$.

We need to define the element $\Phi(g)$ of S_n, but to define this, we need to define $\sigma(1), \ldots, \sigma(n)$. We need to define $\Phi(g)(i) \in S$ for all $g \in G, i \in S$.

We can just take $\Phi(g)(i) \overset{\text{def}}{=} g \star i$.

We check that $\Phi(g) \in S_n$. Fix g, then $\{g \star i\} = S$, so $\Phi(g)$ is a bijection. We check that $\Phi : G \to S_n$ is a homomorphism, i.e. $\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2)$. Since all of these are elements of S_n we only need to show that they agree on where to send each element of S.

$\Phi(g_1 g_2)(i) = (g_1 g_2) \star i = g_1 \star (g_2 \star i) = g_1 \star (\Phi(g_2)(i)) = \Phi(g_1)(\Phi(g_2)(i)) = \Phi(g_1) \circ \Phi(g_2)(i)$.

We now show that Φ is a bijection. To show surjectivity, we note that $g \star i \overset{\text{def}}{=} \Phi(g)(i) \in S$ is a group action, since $1 \star i = \Phi(1)(i) = i$ for all i, and $(g_1 g_2) \star i = g_1 \star (g_2 \star i)$ from $(g_1 g_2) \star i = \Phi(g_1 g_2)(i) = \Phi(g_1) \circ \Phi(g_2)(i) = \Phi(g_1)(g_2 \star i) = g_1 \star (g_2 \star i)$. So Φ is surjective. For injectivity, suppose that $\star_1 \star_2$ are actions of G on S such that $f(\star_1) = f(\star_2)$. By definition of f, $f(\star_1)(g)(i) = g \star_1 i$ and $f(\star_2)(g)(i) = g \star_2 i$, so $\star_1 = \star_2$, as desired. □

§14 March 5, 2020

Remark 14.1. We can extend this idea to group actions on sets other than $\{1, \ldots, n\}$. In general, if S is a non-empty set, define $\text{Perm}(S)$ to be the set of all bijections from $S \to S$ with the group action being composition.

Let G be a group. Then there is a bijection between actions of G on S and the homomorphisms from G to $\text{Perm}(S)$. Note that if $S = \{1, \ldots, n\}$, then $\text{Perm}(S) = S_n$.

§14.1 Faithful Group Actions

Definition 14.2. Let G be a group, S a set, and $\star$ be an action of G on S. $\star$ is a **faithful** group action if $f(\star)$ produces an injective homomorphism from G to $\text{Perm}(S)$.

$\Phi : G \to \text{Perm}(S)$ homomorphism. Φ injective $\iff \ker \Phi - \{1\}$. $\ker \Phi =$ all elements of g that get sent to $\text{id} \in \text{Perm}(S)$.

$\star$ faithful $\iff$ $f(\star)$ is injective $\iff \ker f(\star) = \{1\}$.

$\ker f(\star) = \{g \in G \mid f(\star)(g) = \text{id}\} = \{g \in G \mid f(\star)(g)(s) = s \forall s \in S\} = \{g \in G \mid g \star s = s \forall s \in S\ \} = \{1\}$. so $\star$ is faithful $\iff$ the only element in G which stabilizes every element in S is 1.

Example 14.3 (Unfaithful)

Let G be a group, S a set, and define the group action $g \star s = s$. Then $\star$ is not faithful, unless G is trivial.

Theorem 14.4 (Cayley's Theorem)

Every finite group is isomorphic to a subgroup of some symmetric group. If the group has n elements, then it is isomorphic to a subgroup of S_n.

Proof. Use the idea of a group action. G acts on itself by left multiplication, so for $s = g$, we have $g \star s = gs$. Note that the orbit of every $s \in S$ is $\mathcal{O}_s = S = G$ since we can choose $g = g's^{-1}$ so that $g \star s = g's^{-1}s = g'$ for $g' \in G$.

Then we have that $\star$ is faithful, since the only $g \in G$ for which $gs = g \star s = s$ is $g = 1$. So using a function f from before, we have that $f(\star) = \Phi$, a homomorphism from G to $\text{Perm}(G)$ that is injective. Applying the first isomorphism theorem on Φ, we have that $G = G/\ker \Phi \cong \text{Im}\, \Phi$, so G is isomorphic to a subgroup of $\text{Perm}(G)$.

If $|G| = n$, then $\text{Perm}(G) \cong S_n$. From $G = \{a_1, \ldots, a_n\}$, we note that the bijections from G to itself (which form $\text{Perm}(G)$) can be transformed to bijections from $\{1, \ldots, n\}$ to itself (which form S_n) by looking at the indices. Thus, G is isomorphic to a subgroup of S_n. □

Remark 14.5. Another important action of G on itself is **conjugation**.

$$g \star s \overset{\text{def}}{=} gsg^{-1}$$

for $s \in S \in G$. The stabilizer of s, $\text{stab}(s)$, is called the **centralizer** of s, which is the set of all g that commutes with s. The orbit $\mathcal{O}_s$ is called the **conjugacy class** of s.

§14.2 p-groups

Definition 14.6. A group G is called a **p-group** if $|G| = p^n$, $n \in \mathbb{Z}_{\geq 1}$ with prime p.

Proposition 14.7 (p-groups Have Non-Trivial Centers)

Every p-group has a nontrivial center.

Proof. Let $s \in Z = \text{center of } G$. Then $Z(s) = G$ and $C(s) = \{s\}$. We have that $1 \in Z$ and $|C(1)| = 1$. We also have that $|G| = |\mathcal{O}_s|\,|\text{stab}(s)| = |C(s)|\,|Z(s)|$ so $p^n = |C(s)|\,|Z(s)|$, implying that $|C(s)| = 1$ or $p \mid |C(s)|$.

Suppose that $Z = \{1\}$. Then $|C(s)| \neq 1$, so $p \mid |C(s)|$. It follows that $p^n = \sum_{\text{conjugacy classes}} |C_i| = |C_1| + \sum_{\text{conjugacy classes without 1}} |C_i| \equiv 1 \pmod{m}$, a contradiction. Thus, G must have a nontrivial center. □

§15 March 24, 2020

Theorem 15.1

Let G be a p-group acting on finite S with $p \nmid |S|$. Then S has a fixed point.

Proposition 15.2 (Groups With Prime Square Orders Are Abelian)

Let $|G| = p^2$. Then G is abelian.

Proof. G is abelian if and only if $Z = \text{center}(G) = G$. Z is well-defined, with $Z \leq G$, so that $|Z| \in \{1, p, p^2\}$. By Proposition 14.7, G is nontrivial, so $|Z| = p$ or p^2. By Proposition 15.2, it suffices to show that $|Z| = p^2$.

Suppose $|Z| = p$. Note that for $g \in Z$, we have that $gx = xg$ for each $x \in G \setminus Z$. Then $Z(x)$ contains x and Z, so $|Z(x)| > |Z| = p$. Since $|Z(x)| \mid |G|$, it follows that $|Z(x)| = p^2$, so $Z(x) = G$. This means that x commutes with every element of G, so $x \in Z$, a contradiction. □

Corollary 15.3

Let $|G| = p^2$. Then G is either cyclic or the product of two cyclic groups of order p.

Proof. If G contains an element of order p^2, then it is cyclic. Otherwise, every non-identity element of G has order p. Let $x, y \in G$ such that $y \notin \langle x \rangle$. By Proposition 9.2, we have that $G \cong \langle x \rangle \times \langle y \rangle$. □

Definition 15.4. Let $H \leq G$. Consider the orbit of H with respect to conjugation by G. The orbit of $[H]$ is the set of **conjugate subgroups** $[gHg^{-1}]$, with $g \in G$. The stabilizer of H for this operation is called the **normalizer** of H, denoted by $N(H)$

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Proposition 15.5 (Properties of the Normalizer)

Let $H \leq G$.

1. $H \trianglelefteq N(H)$.
2. $H \trianglelefteq G \iff N(H) = G$.
3. $|H| \mid |N(H)|$ and $|N| \mid |G|$.

§16 March 26, 2020

§16.1 Sylow Subgroups

Definition 16.1. A subgroup H of G is called a **Sylow p-subgroup** if it has order p^e, where p is a prime such that $p^e || |G|$.

Remark 16.2. Sylow p-groups are p-groups, but p-groups are not necessarily Sylow p-groups.

Theorem 16.3 (First Sylow Theorem)
Let G be a finite group with prime $p \mid |G|$. Then G contains a Sylow p-group.

Proof. □

Example 16.4
If G has order 6, then G contains subgroups of orders 2 and 3.

Theorem 16.5 (Second Sylow Theorem)
Let G be a finite group with prime $p \mid |G|$.

1. All Sylow p-subgroups are conjugate subgroups.
2. Every p-subgroup of G is a subgroup of a Sylow p-sbgroup.

Remark 16.6. The previous theorem tells us that if A and B are Sylow p-subgroups, then there $gAg^{-1} = B$. Also, we have that for each p-group A with order p^k, there exists a Sylow p-group B with oder p^e, where $e \geq k$ and $A \leq B \leq G$.

Theorem 16.7 (Third Sylow Theorem)
Let G be a finite group with prime $p \mid |G|$. Let S be the number of distinct Sylow p-groups, then

1. $s \mid m$, where $|G| = p^e m$.
2. $s \equiv 1 \pmod{p}$.

Corollary 16.8 (Existence of Element With Order p)
If prime p divides the order of finite group G, then there is an element $x \in G$ of order p.

Proof. The First Sylow Theorem tells us that there is a subgroup H of G of order p^e, $e \geq 1$. H cannot be trivial, since $|H| > 1$. So there is some $x \in H$ with $x \neq 1$. Then $\langle x \rangle \leq H$, so $|\langle x \rangle| = p^k$ for some k. It follows that $x^{p^{k-1}}$ has order p, as desired. □

Corollary 16.9 (Unique Normal Sylow p-subgroups)
If prime p divides the order of finite group G and H is a Sylow p-subgroup, then H is normal if and only if there is exactly one Sylow p-subgroup.

Proof. We have that if H is normal, then $gHg^{-1} = H$. The Second Sylow Theorem implies that if a Sylow p-subgroup is normal, then there is only 1 Sylow p-subgroup. □

Proposition 16.10
We have the following.

1. Every group of order 15 is cyclic.
2. There are 2 isomorphism classes of groups of order 6.
3. There are 2 isomorphism classes of groups of order 21.

Proof. 1. There exists a Sylow 3-subgroup H and a Sylow 5-subgroup K. Since $15 = 3^1 \cdot 5^1$, it follows that $|H| = 3, |k| = 5$. Let s_3 and s_5 denote the number of Sylow 3 and 5 subgroups. Then $s_3 \mid 5$ and $s_5 \mid 3$. From the Third Sylow Theorem, we must have $s_3 = s_5 = 1$, so H and K are normal subgroups of G. Let $x \in H$ and $y \in K$. By Proposition 9.2, we have that $G \cong \langle x \rangle \times \langle y \rangle$. Thus, G is also cyclic. □

2. By the First Sylow Theorem, there is a subgroup H of G of order 2 and a subgroup K of G of order 3. Let s_2 and s_3 denote the number of Sylow 2- and 3-subgroups. The Third Sylow Theorem tells us that $s_2 \mid 3$ and $s_2 \equiv 1 \pmod 2$, so we can't rule out $s_2 = 1$ or 3. However, we also have that $s_3 \mid 2$ and $s_3 \equiv 1 \pmod 3$, so that $s_3 = 1$. By Corollary 16.9, we have that $K \trianglelefteq G$. We consider two cases:

   Case 1: There is only 1 Sylow 2-subgroup. Then $H \trianglelefteq G$, so $G \cong H \times K \cong C_2 \times C_3 \cong C_6$.

   Case 2: There are 3 Sylow 2-subgroups. Let $S = \{H_1, H_2, H_3\}$. G acts on S by conjugation. By the permutation representation theorem, there is a bijection between the actions of G on S and the homomorphism $\phi : G \to \text{Perm}(S)$, where $\text{Perm}(S) = S_3$ in this case. To show that ϕ is an isomorphism, it suffices to show that ϕ is either injective or surjective (since $|G| = |S_3|$). Here we show that ϕ is injective by showing that $\ker \phi = \{1\}$, i.e. that the action of G on S is faithful.

3.

□

§17 March 31, 2020

Lemma 17.1 (Stabilizer Order Divides Set for Left Multiplication)
Let U be a subset of a group G. The order of $\text{stab}(U)$ for the group action of left multiplication by G on the set of its subsets divides both $|U|$ and $|G|$.

Proof. If H is a subgrouo of G, then the H-orbit of an element u of G for left multiplication by H is the right coset Hu. Let H be the stabilizer of U. Then multiplication by H

permutes the elements of U,, so U is partitioned into H-orbits, which are right cosets. Each coset has order $|H|$, so $|H| \mid |U|$. Because H is a subgroup, $|H| \mid |G|$. □

Lemma 17.2

Let $n = p^e m$, $e \geq 1$, $p \nmid m$. Let N be the number of distinct subsets of $\{1, \ldots, n\}$ of size p^e. Then $p \nmid N$.

Proof. We have that $N = \binom{n}{p^e} = \dfrac{n(n-1)\ldots(n-p^e+1)}{p^e(p^e-1)(p^e-2)\ldots 1}$. $N \not\equiv 0 \pmod{p}$ because every time p divides $(n-k)$ in the numerator, it also divides (p^e-k) in the denominator the same number of times, i.e. if we write k in the form $k = p^i \ell$, $p \nmid \ell$, then $i < e$. So $p^e - k$ and $n - k = p^e m - k$ are both divisible by p^i but not p^{i+1}. □

We now prove the Sylow Theorems

Proof of First Sylow Theorem. Let $|G| = p^e m$ and S be the set of all subsets of G of order p^e. We will show that at least one of these is a Sylow p-subgroup. Instead of finding this directly, we will find an element U os S ($U \subseteq G, |U| = p^e$) so that $\text{stab}(U)$ has size p^e, $\text{stab}(U) \leq G$. This means that $\text{stab}(U)$ is a Sylow p-subgroup.

We have that $|S| = \sum_{\text{orbits } O} |O|$. By lemma 2, $p \nmid |S|$. Thus, there must be some element $U \in S$ such that $p \nmid |O_U|$. Let $H = \text{stab}(U)$. Then $|H| \mid |U|$, so $|H| = p^i$ for some $0 \leq i \leq e$. By the counting formula, $|G| = |\text{stab}(U)|\,|O_U|$, so $p^e m = |H|\,|O_U|$. Since $p \nmid |O_U|$, it follows that $|H| = p^e$, so H is a Sylow p-subgroup. □

Proof of Second Sylow Theorem. Let $K \leq G$, K is a p-group, i.e. $|K| = p^i$ for some $i \geq 1$. Let H be a Sylow p-subgroup, which exists by the First Sylow Theorem.

We claim that there is some $g \in G$ so that $K \leq gHg^{-1}$, where gHg^{-1} is s Sylow p-subgroup because it has size p^e. If this clai holds, then both parts of the theorem immediately follows.

We use left multiplication as a group action to prove the claim. Let S be the set of left cosets of H in G.

This is transitive, since for left cosets aH and bH, we have $(ba^{-1}) * (aH) = bH$. p does not divide the order of S, and S contains an element c whose stabilizer is H.

We restrict the group action of G on S to the p-group K. Let $c = H$. Since S is transitive, there is some $g \in G$ such that $c' = g * c$. Then $\text{stab}(c') = g\text{stab}(c)g^{-1}$. Since $\text{stab}(c) = H$, then $\text{stab}(c') = gHg^{-1}$. Since K fixes c' by the Fixed Point Theorem, it follows that $K \leq gHg^{-1}$, as desired. □

§18 April 2, 2020

Proof of Third Sylow Theorem. Let $|G| = p^e m$. Let s denote the number of Sylow p-subgroups. The Second Sylow Theorem tells us that the group action of G on the set S of Sylow p-subgroups is transitive. The stabilizer of a particular Sylow p-subgroup $[H]$ is the normalizer $N = N(H)$ of H. By the counting formula, we have that $[G : N] = s$. Since $H \leq N$ and $[G : H] = m$, then $s \mid m$.

We use group actions of G on S again. Fix a Sylow p-subgroup H, which exists by the First Sylow Theorem. H acts on S by conjugation. Then we have that $s = |S| =$

$\sum_{H\text{-orbts}O} |O|$. For each $x \in S$, the counting formula tells us that $p^e = |H| = |O(x)|\,|\text{stab}(x)|$, so $|O(x)| = |C(x)|$ divides p^e. Then either $|O(x)| = 1$ or $p \mid |O(x)|$.

Note that the H-orbit $[H]$ has order 1. Since H is a p-group, the order of any H-orbit is a power of p. To show that $s \equiv 1 \pmod{p}$, we show that no other element of S aside from $[H]$ is fixed by H.

Suppose that H' is a Sylow p-subgroup and that conjugation by H fixes $[H']$. Then H is contained in the normalizer N' of H', so both H and H' are Sylow p-subgroups of N'. By the second Sylow theorem, the Sylow p-subgroups of N' are conjugate subgroups of N'. But H' is a normal subgroup of N'. Thus, $H' = H$, as desired. □

§18.1 Rings

Definition 18.1. A **ring** $(R, +, \times)$ is a set R along with binary operations $+ : R \times R \to R$ and $\times : R \times R \to R$, which are usually denoted as addition and multiplication, with the following properties:

1. $(R, +)$ is an abelian group with identity denoted by 0.
2. Multiplication is commutative and associative, with identity denoted by 1.
3. **distributive law**. For all $a, b, c \in R$, $(a + b)c = ac + bc$.

Remark 18.2. $(R, \times)$ is not necessarily a group since R may not necessarily contain multiplicative inverses.

Definition 18.3. A **field** is a ring in which every element other than 0 has a multiplicative inverse.

Definition 18.4. An **ordered field** is a field along with an order $<$ that interacts in the usual way with addition and multiplication.

Remark 18.5. An ordered field in which every subset that is bounded below has a greatest lower bound is $\mathbb{R}$.

Example 18.6 (Gauss Integers)
The Gauss integers: $\{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a ring under usual complex addition and multiplication.

Definition 18.7. Let R be a ring. Then $r \in R$ is a **unit** if it has a multiplicative inverse.

Remark 18.8. As before, the identities 0 for addition and 1 for multiplication are unique.

Remark 18.9. Is it possible for $0 = 1$? Yes, consider the trivial ring $R = \{0\}$. Are there any non-trivial examples? It turns out that the answer is no.

Proof. Suppose R is a ring with $0 = 1$. Observe that $0a = 0$ for every $a \in R$ since $0 = 0a - 0a = (0 + (-0))a = 0a$. Then if $0 = 1$, we have $a = 1a = 0a = 0$ for every $a \in R$, a contradiction. □

Remark 18.10. If b is the additive inverse of a, then bc is the additive inverse of ac for all $c \in R$.

Proof. $ac + bc = bc + ac = (b + a)c = 0c = 0$. □

§19 April 7, 2020

§19.1 Polynomial Rings

Definition 19.1. Given a ring R, the **polynomial ring** in one variable with coefficients in R is all **formal finite** polynomials with coefficients in R.

$$R[x] = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0.$$

Remark 19.2. In the above definition, we don't think of polynomials as functions. Instead, x is just a placeholder to tell us the index of the coefficient.

Fact 19.3. The $n+1$ elements $(a_n, a_{n-1}, \ldots, a_0)$, $a_n \neq 0$ of R uniquely determines a polynomial in $R[x]$.

Definition 19.4. A polynomial in a ring R in one variable is a countable ordered sequence $(a_0, a_1, a_2, \ldots)$ of elements in R so that all $a_1 = 0$ except for finitely many.

Example 19.5

The polynomial $f(x) = x^2 + 1$, $R = \mathbb{Z}$ can be expressed as $(1, 0, 1, 0, 0, \ldots)$.

Example 19.6

Consider $R = \mathbb{F}_2$. There are infinitely many polynomials in $R[x]$. These are all the binary sequences possible.

Definition 19.7. A **monomial** is a polynomial of type x^i for some $i \geq 0$, i.e. a sequence of coefficients with exactly one 1.

Definition 19.8. The **degree** of a polynomial is the largest exponent of x that carries a non-zero coefficient. The **leading coefficient** is the non-zero coefficient of the highest index.

Fact 19.9. With the usual polynomial definitions for addition and multiplication, $R[x]$ is a ring.

Theorem 19.10 (Polynomial Division)

Let R be a ring, and $f, g \in R[x]$. If f is monic, then there are unique polynomials $q(x)$ and $r(x)$ in $R[x]$ so that

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

with $\deg r < \deg f$. In particular, $f \mid g$ if and only if $r = 0$.

Proof. Induction on $\deg g$. □

Corollary 19.11

$g(x)$ is divisible by $x - \alpha$, $\alpha \in R$ if and only if $g(\alpha) = 0$.

Proof. $x - \alpha$ is monic, so $g(x) = q(x)(x-\alpha) + r(x)$ with $\deg r < \deg f = 1$, so r must be a constant. r is 0 if and only if $x - \alpha \mid g(x)$. $g(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha) = \alpha$. □

Definition 19.12. $R[x_1, \ldots, x_n]$ is the set of polynomials with coefficients in R in n variables.

§20 April 9, 2020

Definition 20.1. A **multi-index** is an n-tuple $i = (i_1, \ldots, i_n)$ with each $i_j \in \mathbb{Z} \geq 0$. Then we can write a monomial symbolically as x^i:

$$x^i = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Then a polynomial $f(x) = f(x_1, \ldots, x_n)$ can be written uniquely in the form

$$f(x) = \sum_i a_i x^i,$$

where i runs through all multi-indices $(i_1, \ldots, i_n)$.

Remark 20.2. An element of $R[x_1, \ldots, x_n]$ is a function from all multi-indices i to R, so that all but finitely many are 0.

§20.1 Subrings

Definition 20.3. A **subring** $(R', +', \times')$ is a ring such that $R' \subseteq R$, $+'$ is $+$ restricted to R', and $\times'$ is $\times$ restricted to R', and

1. **closure**. R' is closed under $+$ and $\times$.
2. **additive inverse**. For every $x \in R'$, the additive inverse of x is in R'.
3. **multiplicative identity**. The multiplicative identity 1 is in R'.

Remark 20.4. $0 \in R'$. Since R' is non-empty, there exists an $x \in R'$, and so $-x$ is also in R'. Since R' is closed under addition, $0 \in R'$.

§20.2 Ring Homomorphism

Definition 20.5. A **ring homomorphism** $\phi : R \to Q$, where R and Q are rings, is a function such that

1. $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
2. $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
3. $\phi(1_R) = 1_Q$.

Example 20.6 (Ring Homomorphism from Integers to Modulo)
$\phi : \mathbb{Z} \to \mathbb{F}_p$: $\phi(x) = \bar{x}$, which is the equivalence class of $x \pmod p$.

Fact 20.7. There is a canonical ring homomorphism $\phi_\alpha : R[x] \to R$ given by evaluating the polynomial, i.e. for $f(x) \in R[x]$, $f(x) = \sum_i a_i x^i$ and

$$\phi_\alpha(f(x)) \stackrel{\text{def}}{=} \sum_i a_i \alpha^i$$

where we let $x = \alpha$.

Example 20.8 (Canonical Ring Homomorphism)

$R = \mathbb{R}$, $\alpha = 2$, and $f(x) = x^2 + x \in R[x]$. Then $\phi_\alpha(f) \stackrel{\text{def}}{=} 2^2 + 2 = 6$.

Proposition 20.9 (Substitution Principle)

Let R and Q be rings, and $\phi : R \to Q$ be a ring homomorphism.

1. For every $\beta \in Q$, there is a unique ring homomorphism $\Phi : R[x] \to Q$ that agrees with ϕ on constant polynomials and satisfies $\Phi(x) = \beta$.
2. More generally, for $\phi_1, \ldots, \phi_n \in Q$, there is a unique homomorphism $\Phi : R[x_1, \ldots, x_n] \to Q$ such that Φ and ϕ agree on constant polynomials and $\Phi(x_i) = \alpha_i$ for each $i = 1, \ldots, n$.

Proof. 1. Suppose that Φ and Φ' exist and satisfies the first property. Fix $f(x) \in R[x]$, $f(x) = \sum_i a_i x^i$. Then $\Phi(f(x)) = \Phi(\sum_i a_i x^i) = \sum_i \Phi(a_i x^i) = \sum_i \Phi(a_i)\Phi(x)^i = \sum_i \Phi(a_i)\beta^i = \sum_i \phi(a_i)\beta^i$, which is the same as $\Phi'(f(x))$. So Φ and Φ' agree on all polynomials in $R[x]$, so they must be equal.

We now construct such a Φ. Given $f(x) = \sum_i a_i x^i \in R[x]$, define $\Phi(f(x)) = \sum_i \phi(a_i)\beta^i$. Then $\Phi(0) = 0 \in Q$. We also check that $\Phi(1) = \phi(a_0)\beta^0 = \phi(a_0) = \phi(1) = 1 \in Q$, and $\Phi(f(x) + g(x)) = \Phi(\sum_i (a_i + b_i)x^i) = \sum_i \phi(a_i + b_i)\beta^i = \sum_i \phi(a_i)\beta^i + \sum_i \phi(b_i)\beta^i = \Phi(f(x)) + \Phi(g(x))$, and that $\Phi(f(x)g(x)) = \Phi(\sum_{i,j} a_i b_j x^{i+j}) = \Phi(f(x))\Phi(g(x))$.

2. Similar to above.

□

§21 April 14, 2020

Fact 21.1. There is a natural homomorphism $i : R \to R[x]$ called the **inclusion homomorphism**.

$$r \in R, \qquad i(r) = r.$$

Fact 21.2. Compositions of homomorphisms yields homomorphisms.

Example 21.3

If $i : Q \to Q[x]$ is the inclusion homomorphism, and $\psi : R \to Q$ is a homomorphism, then for homomorphism $\phi \stackrel{\text{def}}{=} i \circ \psi$ with $\phi : R \to Q[x]$. The substitution principle tells us that there is a unique extension of ϕ to a homomorphism $\Phi : R[x] \to S[x]$ that ends $x \mapsto x$.

Proposition 21.4

There is a unique isomorphism $\Phi : R[x, y] \to R[x][y]$, which is the identity on R and sends $x \mapsto x$, $y \mapsto y$.

Proof. Note that R is a subring of $R[x]$ and $R[x]$ is a subring of $R[x][y]$, so there are inclusion homomorphisms $R \to R[x]$ and $R[x] \to R[x][y]$. Composing these gives us a homomorphism from $R \to R[x][y]$. The substitution principle tells us that there is a unique homomorphism $\Phi : R[x, y] \to R[x][y]$ that agrees with ϕ on constant polynomials and takes x, y to wherever we want. So we can send these variables to themselves. □

Remark 21.5. Let $\phi : \mathbb{Z} \to R$ be a homomorphism. Then ϕ is uniquely determined by $\phi(1)$, since $\phi(n) = \phi(1 + \cdots + 1) = n\phi(1)$ and $\phi(-n) = -n\phi(1)$ and $\phi(0) = 0$.

§21.1 Ideals

Definition 21.6. An **ideal** I is a subset of R such that

1. I is closed under addition.
2. $rs \in I$ for $s \in I$, $r \in R$.

Definition 21.7. Let R, Q be rings, and $\phi : R \to Q$ be a homomorphism. The **kernel** of ϕ is $r \in R, \phi(r) = 0_Q$.

Remark 21.8. The kernel can't be a subring for a nonzero ring Q.

Remark 21.9. The kernel is closed under addition since $\phi(a+b) = \phi(a)+\phi(b) = 0+0 = 0$, so $a + b$ is in the kernel if a and b are. Similarly, for $r \in R, s \in \ker \phi$, we have that $\phi(rs) = \phi(r)\phi(s) = \phi(r) \cdot 0 = 0$, so $rs \in \ker \phi$.

Remark 21.10. Alternate definition for idelas: I is nonempty, and a linear combination $r_1 s_1 + \cdots + r_k s_k$ of elements $s_i \in I$ with coefficients $r_i \in R$ is in i.

Definition 21.11. The **principal ideal** generated by an element $a \in R$ is the set of all products of a.

$$(a) = aR = Ra = \{ra \mid r \in R\}.$$

If I is an ideal and $a \in I$, then $(a) \subseteq I$.

Definition 21.12. The **unit ideal** is defined by $(1) = R = \{r \cdot 1 \mid r \in R\}$. The **zero ideal** is defined by $(0) = \{0\} = \{r \cdot 0 \mid r \in R\}$.

Definition 21.13. An ideal I is **proper** if $I \neq (0)$ and $I \neq (1)$.

Definition 21.14. An ideal I is generated by a subset $S \subseteq R$ if $S \subseteq I$ and every element $a \in I$ can be written as $a = r_1 s_1 + \cdots + r_n s_n$ for some $r_1, \ldots, r_n \in R$ and $s_1, \ldots, s_n \in S$.

Example 21.15

Some generated ideals.

1. $R[x] = (1)$ is generated by $R[x]$.
2. I is the set of all polynomials with $a_0 = 0$. Then I is an ideal generated by x.

Proposition 21.16 (Fields and Ideals)

Let $\mathbb{F}$ be a field.

1. The only ideals of $\mathbb{F}$ are (0) and $(1) = \mathbb{F}$.
2. A ring that has exactly two ideals is a field.

Proof. 1. Suppose that I is an ideal of $\mathbb{F}$. If $I \neq (0)$, then there exists $x \in I$ with $x \neq 0$. Since $\mathbb{F}$ is a field, there is some $y \in \mathbb{F}$ such that $xy = 1$. Since $xy \in I$, so $1 \in I$, so $(1) \subseteq O$, so $\mathbb{F} \subseteq O$. Thus, $I = \mathbb{F} = (1)$. □

2. Suppose that R is a ring with this property. Let $a \in R, a \neq 0$. We will show that a has a multiplicative inverse in R. Consider (a). We know that this is either A or B, the two ideals of R. (0) and (1) are always ideals of R, so let $A = (0)$, $B = (1)$. If $A = B$, then R is the zero ring, which only has one element, contradicting the assumption that R has two ideals. Consider the principal ideal (a). It is not the zero ideal because it contains a. Thus, it is the unit ideal. The elements of (a) are multiples of a, so 1 is a multiple of a. Thus, a has a multiplicative inverse in R, as desired.

□

§22 April 16, 2020

Corollary 22.1

Every homomorphism $\phi : \mathbb{F} \to R$ from a field $\mathbb{F}$ to a nonzero ring R is injective

Proof. The kernel of ϕ is an ideal of $\mathbb{F}$. By the previous proposition, the kernel is either (0) or (1). If $\ker \phi$ were the unit ideal (1), then ϕ would be the zero map. But the zero map isn't a homomorphism when R isn't the zero ring. Thus, $\ker \phi = (0)$, and ϕ is injective. □

Proposition 22.2

The ideals of $\mathbb{Z}$ are $n\mathbb{Z}$, and they are principal ideals.

Proof. An ideal of the ring $\mathbb{Z}$ of integers will be a subgroup of the additive group $\mathbb{Z}^+$, which takes the form $n\mathbb{Z}$. □

Proposition 22.3

Let $\mathbb{F}[x]$ be the ring of polynomials in 1 variable. If I is an ideal of $\mathbb{F}[x]$, then I is principal and is generated by the unique polynomial f in I which is a monic polynomial of least degree.

Proof. Suppose I is not the zero ideal. Then there exists a non-zero polynomial f in I of minimal degree since for $f \in I, f \neq 0$, either f has minimal degree, or there is some $f' \in I$ of degree less than $\deg f$. We can repeat this process to obtain the desired f, since the process must terminate after a finite number of steps. Let the leading coefficient of f be $r \neq 0$. Consider $r^{-1}f$, where r^{-1} exists since $\mathbb{F}$ is a field.

Thus, we may assume without loss of generality, that f is a monic non-zero polynomial of minimal degree. Then f is unique, since if f_1 satisfies the same properties, then $f - f' \in I$, where $\deg(f - f') < \deg f$, which implies that $f - f'$ is the zero polynomial since f has minimal degree, as desired.

We now show that $(f) = I$. $(f) \subseteq I$ holds since $f \in I$ and since I is an ideal. To show that $I \subseteq (f)$, consider an element $g \in I$. Since f is monic and nonzero, then $g = fq + r$, for unique q, r with $r = 0$ and $\deg r < \deg r$. $r \neq 0$ contradicts the minimality of the degree of f. $r = 0$ yields that g is a multiple of f. Thus, $I \subseteq (f)$, as desired. □

Definition 22.4. The **characteristic** of a ring R is the non-negative integer n that generates the kernel of the homomorphism $\phi : \mathbb{Z} \to R$. If $n = 0$, then the characteristic is zero, and all positive multiples of 1 in R are nonzero. Otherwise, n is the smallest positive integer such that $n \cdot 1$ is 0 in R.

§23 April 21, 2020

§23.1 Quotient Rings

Definition 23.1. Let I be an ideal of a ring R. The cosets of the additive subgroup I^+ of R^+ are the subsets $a + I$. Thus, $\bar{R} = R/I$ is a group under addition. In fact, this is a ring.

Definition 23.2. The **product ring** $R \times R'$ is the set $\{(x, y) \mid x \in R, y \in R'\}$, where addition and multiplication occurs element-wise.

Proposition 23.3 (Decomposing Ring Using Idempotent Element)

Let e be an idempotent element of ring R.

1. Let $e' = 1 - e$. Then $e + e' = 1$ and $ee' = 0$.
2. $eR = (e)$ is a ring with identity e, and the map $f : R \to (e)$ given by $f(x) = ex$ is a homomorphism.
3. The ideal eR is a subring of R if and only if $e = 1$ and $e' = 0$.
4. R is isomorphic to $eR \times e'R$.

Proof. 1. $(e')^2 = (1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = e'$. So $ee' = e(1 - e) = e - e = 0$.

2. (e) is closed under addition and multiplication. It is easy to see that $f(a+b) = ea + eb = f(a) + f(b)$ and $f(ab) = eab = e^2ab = f(a)f(b)$, and finally, $f(1) = e$ is the identity in eR.

3. If $e = 1$, then (e) contains 1.

4. The map $\phi : R \to eR \times e'R$ defined by $\phi(x) \stackrel{\text{def}}{=} (ex, e'x)$ is a homomorphism since $x \rightsquigarrow ex$ and $e \rightsquigarrow e'x$ are homomorphisms. $\phi(x) = (0,0) \iff x = 0$, so ϕ is injective. To show that ϕ is surjective, let $(u, v) \in eR \times e'R$ and let $u = ex$ and $v = e'y$. Then $\phi(u + v) = (e(ex + e'y), e'(ex + e'y)) = (u, v)$. Thus ϕ is also surjective.

□

Example 23.4
In $\mathbb{Z}/6\mathbb{Z}$, $\bar{3}$ is idempotent

§23.2 Adjoining Elements

Definition 23.5. If R is a subring of ring Q, then Q is called a **ring subring** of R.

Example 23.6
Let $Q = R[x]$. Then R is a subring of Q corresponding to constant polynomials.

Definition 23.7. Let R be a ring. Then we can adjoin an element α to R to obtain a ring containing α and the elements of R by considering $R[\alpha]$.

§24 April 23, 2020

Definition 24.1. A ring R is an **integral domain** if it is not trivial, and if for every $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

Theorem 24.2 (Correspondence Theorem)
Let $\phi : R \to R'$ be a surjective ring homomorphism, and let $I = \ker \phi$. There is a bijection between the set of ideals of R that contain I and the set of ideals of R'.

Sketch of proof. Let Q be an ideal of R that contains I. Then we send Q to $\phi(Q)$. Similarly, if Q' is an ideal of R', then $\phi^{-1}(Q') = \{r \in R : \phi(r) \in Q'\}$. □

Fact 24.3. If Q is an ideal of R containing I and $Q' = \phi(Q)$, then $R/Q \cong R'/Q'$.

Definition 24.4. A **maximal ideal** M of ring R is an ideal that isn't equal to R and isn't contained in any ideal other than M and R.

Proposition 24.5 (Maximal Ideals and Fields)
Let $\phi : R \to R'$ be a surjective ring homomorphism with kernel I.

1. R' is a field if and only if I is a maximal ideal.
2. An ideal Q of R is maximal in R if and only if $\bar{R} = R/Q$ is a field.
3. The zero ideal of a ring R is maximal if and only if R is a field.

Proof. 1. A ring is a field if it has exactly 2 ideals, so by the Correspondence Theorem, $\operatorname{im}\phi$ is a field if and only if there are exactly 2 ideals that contain kernel I. This holds if and only if I is a maximal ideal.

2. Using the surjective canonical map $f : R \to R/Q$ and the result of part (a), R/Q is a field if and only if $\ker f = Q$ is maximal.

3. From part (b), (0) is maximal if and only if $R/(0)$ is maximal if and only if $R/(0)$ is a field, and $R/(0) \cong R$.

□

Proposition 24.6 (Prime Ideals Are the Only Maximal Ideals in $\mathbb{Z}$)
The maximal ideals of $\mathbb{Z}$ are (p), where p is prime.

Proof. Let I be an ideal of $\mathbb{Z}$, and let $I = (n)$. Suppose that I is maximal and n is not prime. There exist 3 cases.

Case 1: $n = 0$. However, (0) is not maximal since $(2) \neq \mathbb{Z}$ and $(0) \subset (2)$.

Case 2: $n = 1$. However, maximal ideals can't be the whole ring, and $(1) = \mathbb{Z}$.

Case 3: $n = ab$ is composite. Since $b > 0$, we have $(n) \subset (a) \subset (1)$, contradicting the assumption that (n) is maximal.

Thus, n must be prime. □

Definition 24.7. A polynomial f with coefficients in a field $\mathbb{F}$ is **irreducible** if it is not constant and can't be written as the product of two non-constant polynomials.

Proposition 24.8 (Prime Polynomials Generate Maximal Ideals)
Let $\mathbb{F}$ be a field. The maximal ideals in $\mathbb{F}[x]$ are the principal ideals generated by the monic irreducible polynomials.

Proof. Let I be a maximal ideal. Since I is an ideal and $\mathbb{F}$ is a field, $I = (f)$ for some unique monomial in I of minimal degree.

Suppose f is reducible. If f is constant, then $(f) = (0)$ or (1), neither of which are maximal. If $f = gh$ for non-constant polynomials g, h, then $(f) \subset (g) \subset \mathbb{F}[x]$, so f is not maximal.

Thus f must be irreducible. Suppose that $(f) \subset M \subset \mathbb{F}[x]$ for some ideal M. Then $M = (g)$ for some unique monomial g of lowest degree in M. From $f = hg + r$, since $f \in M$, then $f = hg$, so f is in the ideal generated by g. If h is constant, then $(f) = (g)$. If g is constant, also impossible. Thus, g, h must both be non-constant, contradicting the assumption that f is irreducible. □

Corollary 24.9

There is a bijection between maximal ideals of the polynomial ring $\mathbb{C}[x]$ and $\mathbb{C}$ given by $z \in \mathbb{C} \rightsquigarrow (x - z) \in \mathbb{C}[x]$.