PMATH 347 - Groups and Rings

Frank Jin

University of Waterloo

frank.jin@uwaterloo.ca

Contents

Section 1

Groups

Subsection 1.1

Notation

Week 1.1

We begin with the following conventions for the course:

- $\mathbb{N} = \{1, 2, 3, ...\}$
- $\mathbb{Z} = \{, ..., -2, -1, 0, 1, 2, ...\}$
- $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$
- $\mathbb{R} =$ the set of all real numbers
- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$
- $\mathbb{Z}_n\{[0], [1], ..., [n-1]\}$ is the set of integers modulo n for $n \in \mathbb{N}$ and $[a] = \{z \in \mathbb{Z} : n \equiv a \pmod{n}\}$ for $0 \leq a \leq n-1$

We use $M_n(\mathbb{R})$ to describe the set of all $n \times n$ matrices over $\mathbb{R}$. Recall the usual matrix addition and multiplications from a linear algebra course.

Subsection 1.2

Groups

Definition 1.1 (Group) Let G be a set and $*$ be an operation on $G \times G$. We say $G = (G, *)$ is a group if it satisfies

1. Closure: If $a, b \in G$, $a * b \in G$
2. Associativity: If $a, b, c \in G$, then $a * (b * c) = (a * b) * c$
3. Identity: There exists an element $e \in G$ such that $a * e = a = e * a$ for all $a \in G$. We call e the identity of G
4. Inverse: For all $a \in G$, there exists $b \in G$ where $a * b = e = b * a$. We call b the inverse of a

Definition 1.2 (Abelian Group) A group G is said to be abelian if $a * b = b * a$ for all $a, b \in G$.

Proposition 1.1 Let G be a group and $a \in G$. Then

1. The identity of G is unique
2. The inverse of a is unique

PROOF

1. Suppose e_1, e_2 are identities of G. Then
$$e_1 = e_1 * e_2 = e_2.$$
2. Suppose b_1 and b_2 are inverses of a. Then
$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2.$$

□

Example $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups with identity 0 and inverse $-a$ for any element a. $(\mathbb{N}, +)$ is not an a group since there is no identity or inverse. $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$, and $\mathbb{C}, \cdot$ are not groups because 0 has no inverse (the identity is 1).

For a set S, we use S^* to denote the subset of S containing all element with multiplicative inverses.

Example We have $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ so $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are abelian groups with identity 1 and the inverse of r given as $\frac{1}{r}$.

Example $(M_n(\mathbb{R}), +)$ is an abelian group. $(M_n(\mathbb{R}), \cdot)$ is not a group because we recall that a matrix A is only invertible if $\det(A) \neq 0$.

Definition 1.3 (General Linear Group) The set $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$ is called the general linear group of degree n over $\mathbb{R}$.

Week 1.2

Note that if $A, B \in GL_n(\mathbb{R})$, then $\det(AB) = \det(A) \cdot \det(B) \neq 0$ so $GL_n(\mathbb{R})$ is closed under $\cdot$. We also recall that associativity is inherent from $M_n(\mathbb{R})$ from linear algebra. The identity matrix I_n has $\det(I_n) = 1 \neq 0$ so $I_n \in GL_n(\mathbb{R})$. Lastly, if $M \in GL_n(\mathbb{R})$, we know $\det(M) \neq 0$ and so M has an inverse M^{-1} where $\det\left(M^{-1}\right) \neq 0$ from linear algebra. This justifies that $GL_n(\mathbb{R})$ is a group. Although, it is not an abelian group since matrix multiplication does not commute in general for $n \geq 2$.

Definition 1.4 (Direct Product) Let $G = (G, *_G)$ and $H = (H, *_H)$ be groups. Their direct product is the set $G \times H$ with the component-wise group operation $*$ given by
$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$
where $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Note that for any groups G and H, their direct product $G \times H$ is a group. In particular, the identity is $(1_G, 1_H)$ where 1_G is the identity of G and 1_H is the identity of H. The inverse of $(g, h) \in G \times H$ is given by $(g, h)^{-1} = (g^{-1}, h^{-1})$. Furthermore, we can show by induction that if $G_1, ..., G_n$ are groups, then so is $G_1 \times ... \times G_n$.

For the sake of brevity, we often denote the identity of a group G by 1 and $g_1 * g_2$ by $g_1 g_2$. Since the inverse of g is unique, we usually write g^{-1} to mean g's inverse.

Proposition 1.2 Let G be a group and $g, h \in G$. Then
1. $(g^{-1})^{-1} = g$
2. $(gh)^{-1} = h^{-1}g^{-1}$
3. $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$
4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

PROOF

1. Since the inverse is unique, and $g^{-1}g = 1$, the result follows.
2. $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = 1$

3 and 4 are left as an exercise. □

Note that in general, it is not true that $gh \in G$ implies $(gh)^n = g^n h^n$.

Proposition 1.3 Let G be a group and $g, h, f \in G$. Then

1. left-right cancellation is satisfied:
   (a) $gh = gf$ implies $h = f$
   (b) $hg = fg$ implies $h = f$
2. Given $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$

PROOF

1. Multiply both sides by g^{-1}
2. Let $x^{-1} = a^{-1}b$ so $ax = a(a^{-1}b) = (aa^{-1})b = b$. If u is another solution, then $au = b = ax$ so cancellation implies $u = x$. Similarly, we can show $y = ba^{-1}$ is the unique solution to $ya = b$.

□

SUBSECTION 1.3

Symmetric Groups

Definition 1.5 (Permutation) Given a nonempty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

We use the notation $S_n = S_{\{1,\dots,n\}}$ for all $n \in \mathbb{N}$. Here is an example of an element in S_3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

We use this notation as follows: the top row is the input, and the bottom row is the output. So if we call this element σ, we have $\sigma(1) = 1$, $\sigma(2) = 3$, and $\sigma(3) = 2$. This is a bijection and thus an element of S_3 as we can see easily that it is one-to-one and onto.

Proposition 1.4 $|S_n| = n!$.

Given $\sigma, \tau \in S_n$, we can compose a third element $\sigma\tau$ given by $x \mapsto \sigma(\tau(x))$. Since σ and τ are bijections, $\sigma\tau$ is a bijection and is contained in S_n too. Week 2.1

Example If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \text{ and } \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

For any $\sigma, \tau \in S_n$, we can then deduce that $\sigma\tau, \tau\sigma \in S_n$. Note that in general, $\sigma\tau \neq \tau\sigma$. We can prove as well that for $\sigma, \tau, \mu \in S_n$, $\sigma(\tau\mu) = (\sigma\tau)\mu$. The identity permutation $\epsilon \in S_n$ can be defined as $\epsilon(x) = x$ for each $x \in \{1, \dots, n\}$. It is clear that for any $\sigma \in S_n$, $\sigma\epsilon = \sigma = \epsilon\sigma$.

Since $\sigma \in S_n$ is a bijection, a unique bijection $\sigma^{-1} \in S_n$ exists called the inverse permutation. Specifically,

$$\sigma^{-1}(x) = y \iff \sigma(y) = x.$$

It follows that $\sigma(\sigma^{-1}(x)) = \sigma(y) = x$ and $\sigma^{-1}(\sigma(y)) = \sigma^{-1}(x) = y$.

Example The inverse of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$ is $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$.

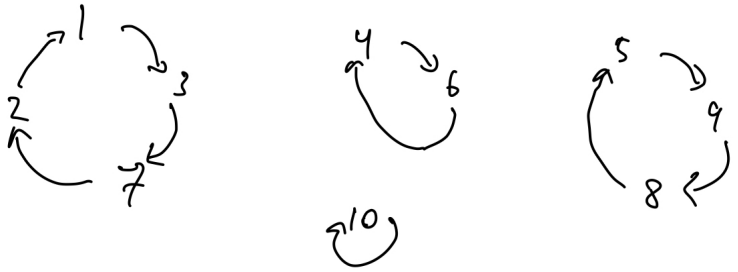
With all of the above being said, we can prove the following proposition:

Proposition 1.5 S_n is a group called the symmetric group of order n.

Consider the permutation $\sigma \in S_{10}$ defined

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix}$$

If we represent the action of σ geometrically, we have:



Thus, σ can be decomposed into one 4-cycle, one 2-cycle, one 3-cycle, and 1 1-cycle. Note that these cycles are all pairwise disjoint and we can represent σ as

$$\sigma = (1\ 3\ 7\ 2)(4\ 6)(5\ 9\ 8).$$

We usually don't write 1-cycles in the representation. Also, we can observe that the order of cycles and starting elements in each cycle do not matter. Although this decomposition in cycle notation is not unique, the elements and their relative ordering within each cycle remains unique.

Theorem 1.6 (Cycle Decomposition) If $\sigma \in S_n$, where $\sigma \neq \epsilon$, then σ is a product of (one or more) disjoint cycles of length ≥ 2. This factorization is unique up to the order of the factors.

A convention we use is that every permutation in S_n can be regarded as a permutation in S_{n+1} by fixing the number $(n+1)$. So, $S_1 \subseteq S_2 \subseteq ...S_n \subseteq S_{n+1} \subseteq ...$

SUBSECTION 1.4

Cayley Tables

For a finite group G, defining its operation by means of a table is sometimes convenient. Given $x, y \in G$, the product xy is the entry of the table in the row corresponding to x and the column corresponding to y. Such a table is called a Cayley table.

Recall that by cancellation, $ax = ay \iff x = y$. So, entries in each row (or each column) must be all distinct.

Example Consider the group $(\mathbb{Z}_2, +)$. The Cayley table is

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Example Consider the group $\mathbb{Z}^* = \{1, -1\}$. Its Cayley table is

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

Note that if we make substitutions of 1 by $[0]$ and -1 by $[1]$, the Cayley tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are the same. We say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are isomorphic: $\mathbb{Z}^* \cong \mathbb{Z}_2$.

Example For $n \in \mathbb{N}$, the cyclic group of order n is defined

$$C_n = \{1, a, a^2, ..., a^{n-1}\}$$

with $a^n = 1$ and $1, a, ..., a^{n-1}$ all being distinct. Write

$$C_n = \langle a = a^n = 1 \rangle$$

and call a a generator of C_n. The Cayley table of C_n is

C_n	1	a	a^2	$\cdots$	a^{n-1}
1	1	a	a^2	$\cdots$	a^{n-1}
a	a	a^2	a^3	$\cdots$	1
a^2	a^2	a^3	a^4	$\cdots$	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a^{n-1}	a^{n-1}	1	a	$\cdots$	a^{n-2}

Proposition 1.7 Let G be a group. Up to isomorphism, we have

1. If $|G| = 1$, $G \cong \{1\}$
2. If $|G| = 2$, $G \cong C_2$
3. If $|G| = 3$, $G \cong C_3$
4. If $|G| = 4$, $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$

K_4 is called the Klein 4-group.

PROOF

1. If $|G| = 1$, then $G = \{1\}$.
2. If $|G| = 2$, then $G = \{1, g\}$ where $g \neq 1$. Then $g^2 = g$ or $g^2 = 1$. If $g^2 = g$, by cancellation, we get $g = 1$ which cannot be the case. So $g^2 = 1$. Writing out the Cayley table, we see it is the same as C_2's Cayley table. Week 2.2
3. If $|G| = 3$, then $G = \{1, g, h\}$ where $g \neq h$ and $g, h \neq 1$. By cancellation, we know $gh \neq g$ and $gh \neq h$. So, $gh = 1$. Similarly, $hg = 1$. Filling out the Cayley table, we see that it is the same as C_3 if we identify h with a^2 and g with a.
4. Left as a question for Assignment 1.

□

Section 2

Subgroups

Subsection 2.1

Subgroups

Definition 2.1 (Subgroup) Let G be a group and $H \subseteq G$ be a subset. If H itself is a group, we say H is a subgroup of G.

Note that since G is a group, for $h_1, h_2, h_3 \in H$, we have commutativity: $h_1(h_2h_3) = (h_1h_2)h_3$.

Definition 2.2 (Subgroup Test) $H \subseteq G$ is a subgroup if all conditions are met:

1. If $h_1, h_2 \in H$, $h_1h_2 \in H$
2. There exists $1_H \in H$ such that $1_H h = h1_H$ for all $h \in H$
3. If $h \in H$, $h^{-1} \in H$

Example Given group G, $\{1\}$ and G are subgroups of G. We can also build a chain of subgroups

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

Example Recall that $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$. Define the special linear group of order n over $\mathbb{R}$ as $SL_n(\mathbb{R}) = (SL_n(\mathbb{R}), \cdot) = \{M \in M_n(\mathbb{R}) : \det(M) = 1\}$. We will show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$:

1. If $A, B \in SL_n(\mathbb{R})$, then $\det(AB) = \det(A)\det(B) = 1$ so $AB \in SL_n(\mathbb{R})$.
2. Consider the identity matrix I_n.
3. If $A \in SL_n(\mathbb{R})$, then $\det\left(A^{-1}\right) = \frac{1}{\det(A)} = 1$.

Definition 2.3 Given group G, we define the center

$$Z(G) = \{z \in G : zg = gz, \forall g \in G\}$$

Note that $Z(G) = G$ if G is abelian.

Example We can show that $Z(G)$ is an abelian subgroup of G. Note $1 \in Z(G)$. Let $y, z \in Z(G)$. Then, for all $g \in G$, we have

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

so $yz \in Z(G)$. Also,

$$zg = gz \iff z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \iff gz^{-1} = z^{-1}g$$

So $z^{-1} \in Z(G)$. We are done by the subgroup test.

Proposition 2.1 Let $H, K \subseteq G$ be subgroups of group G. Then

$$H \cap K = \{g \in G : g \in H \wedge g \in K\}$$

is also a subgroup of G.

Proposition 2.2 (Finite Subgroup Test) If H is a finite and non-empty subset of group G, H is a subgroup if and only if H is closed under its operation.

PROOF The forward direction is obvious. For the backward, let $h \in H$. Since H is closed, $h, h^1, h^2, ... \in H$. Since H is finite, then not all of these elements are distinct: specifically, for some $n, m \in \mathbb{N}$, $h^{n+m} = h^n$. By cancellation, $h^m = 1$ so $1 \in H$. Also, $1 = h^{m-1}h$ so h^{m-1} is the inverse of h. □

SUBSECTION 2.2

Alternating Groups

Recall that for $\sigma \in S_n$, where $\sigma \neq \epsilon$, σ can be decomposed uniquely up to its order as disjoint cycles of length ≥ 2.

Definition 2.4 (Transposition) A transposition $\sigma \in S_n$ is a cycle of length 2, e.g. $\sigma = (a, b)$ with $a, b \in [n]$ where $a \neq b$.

Consider $(1\ 2\ 4\ 5) \in S_5$. Also, consider the composition $(1\ 2)\,(2\ 4)\,(4\ 5)$. We can compute this as Week 2.3

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \\ 1 & 4 & 3 & 5 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

(We compute row-by-row from right to left in the composition, e.g. first swap 4 and 5)

We see from this example that $(1\ 2)\,(2\ 4)\,(4\ 5) = (1\ 2\ 4\ 5)$.

Another equal composition (show this as an exercise) is

$$(2\ 3)\,(1\ 2)\,(2\ 5)\,(1\ 3)\,(2\ 4) = (1\ 2\ 4\ 5)$$

Therefore, we see that factorizations into transpositions are not unique.

Theorem 2.3 (Parity Theorem) If a permutation σ has 2 factorizations $\sigma = \gamma_1 ... \gamma_r = \mu_1 ... \mu_s$, where each γ_i and μ_j is a transposition, then $r \equiv s \pmod 2$.

PROOF Bonus Assignment 2. □

Definition 2.5 A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By the parity theorem, this definition is well-defined.

Theorem 2.4 For $n \geq 2$, let A_n denote the set of all even permutations in S_n. We have:

1. $\epsilon \in A_n$
2. If $\sigma, \tau \in A_n$, $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$
3. $|A_n| = \frac{1}{2}n!$

From (1) and (2), we see A_n is a subgroup of S_n, called the alternating group of order n.

PROOF

1. We can write $\epsilon = (1\ 2)(1\ 2)$, so ϵ is even.
2. If $\sigma, \tau \in A_n$, write $\sigma = \sigma_1 ... \sigma_r$ and $\tau = \tau_1 ... \tau_s$ where σ_i and τ_j are transpositions, and r, s are even. Then $\sigma\tau = \sigma_1 ... \sigma_r \tau_1 ... \tau_s$ is a product of $(r+s)$ transpositions, which is even. Also, note that since σ_i is a transposition, $\sigma_i^2 = \epsilon$ so $\sigma_i^{-1} = \sigma_i$. It follows that
$$\sigma^{-1} = (\sigma_1 ... \sigma_r)^{-1} = \sigma_r^{-1} ... \sigma_1^{-1} = \sigma_r ... \sigma_1$$
which is an even permutation.
3. Let O_n denote the set of odd permutations in S_n. So, $S_n = O_n \cup A_n$ and the parity theorem implies that $A_n \cap O_n = \emptyset$. Since $|S_n| = n!$, to prove $|A_n| = \frac{1}{2}n!$ it suffices to show that $|A_n| = |O_n|$. We will find a bijection between the two sets. Let $\gamma = (1\ 2)$ and define $f : A_n \to O_n$ as $f(\sigma) = \gamma\sigma$. Since σ is even, the $\gamma\sigma$ is odd. This map is thus well-defined. First, to show that f is one-to-one, consider $\gamma\sigma_1 = \gamma\sigma_2$. By cancellation, we have $\sigma_1 = \sigma_2$. Next, we show f is onto. Consider an arbitrary $\tau \in O_n$. Then, $\sigma = \gamma\tau \in A_n$ and $f(\gamma\tau) = \gamma(\gamma\tau) = \gamma^2\tau = \epsilon\tau = \tau$. Therefore, since we have shown that an element in A_n exists mapping to τ, then f is onto. We have successfully shown that f is a bijection, so $|A_n| = \frac{1}{2}n!$.

□

SUBSECTION 2.3

Order of Elements

Given a group G and $g \in G$, we use the notation $\langle g \rangle$ to denote

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\} = \{..., g^{-2}, g^{-1}, g^0, g^1, g^2, ...\}.$$

Note that $g^0 = 1 \in \langle g \rangle$. Also, if $x = g^m$ and $y = g^n$ are elements of $\langle g \rangle$ where $m, n \in \mathbb{Z}$, then $xy = g^{n+m} \in \langle g \rangle$ as well. We see the inverse $x^{-1} = g^{-m} \in \langle g \rangle$ too, so by the subgroup test, we have shown that $\langle g \rangle$ is a subgroup of G.

Proposition 2.5 If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Definition 2.6 (Cyclic Subgroup) Let G be a group and $g \in G$. We call $\langle g \rangle$ the cyclic subgroup of G generated by g. If $G = \langle g \rangle$ for some $g \in G$, then G is a cyclic group and g is a generator of G.

Example Consider $(\mathbb{Z}, +)$. Note that for all $k \in \mathbb{Z}$, $k = k \times 1$. Thus, $(\mathbb{Z}, +) = \langle 1 \rangle$. Similarly, -1 is a generator of $(\mathbb{Z}, +)$. We observe that for any $n \in \mathbb{Z}$ with $n \neq \pm 1$, there exists no $k \in \mathbb{Z}$ such that $kn = 1$. So, ± 1 are the only generators for the group.

Let G be a group and $g \in G$. Suppose that there exists a non-zero $k \in \mathbb{Z}$ such that $g^k = 1$. Then, $g^{-k} = (g^k)^{-1} = 1$. Thus, we can assume that $k \geq 1$. Then, by the well-ordering principle, there exists the smallest positive integer n such that $g^n = 1$, if such a k exists.

Definition 2.7 (Order) Let G be a group and $g \in G$. If n is the smallest positive integer where $g^n = 1$, the order of g is n, denoted $o(g) = n$. If no such n exists, then g has infinite order: $o(g) = \infty$

Proposition 2.6 Let G be a group and $g \in G$ satisfying $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$, we have

1. $g^k = 1 \iff n|k$
2. $g^k = g^m \iff k \equiv m \pmod{n}$
3. $\langle g \rangle = \{1, g, ..., g^{n-1}\}$ where $1, g, ..., g^{n-1}$ are all distinct. In particular, $|\langle g \rangle| = o(g)$

PROOF

1. ($\Leftarrow$) Let $n|k$ meaning $nz = k$ for some $z \in \mathbb{Z}$. Then $g^k = g^{nz} = (g^n)^z = 1^z = 1$.

   Week 3.1

   ($\Rightarrow$) By division algorithm, write $k = qn + r$ where $0 \leq r < n$ and $q, r \in \mathbb{Z}$. Since $g^k = g^n = 1$, we have

   $$g^r = g^{k-nq} = g^k (g^n)^{-q} = 1(1)^{-q} = 1.$$

   Since $0 \leq r < n$, and $o(g) = n$, then r must equal 0 so $n|k$.

2. Note $g^k = g^m \iff g^{k-m} = 1$. By (1), $n|(k-m)$ so $k \equiv m \pmod{n}$.

3. It follows from (2) that $1, g, ..., g^{n-1}$ are all distinct. Clearly, $\{1, g, ..., g^{n-1}\} \subseteq \langle g \rangle$. To prove $\langle g \rangle \subseteq \{1, g, ..., g^{n-1}\}$, let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ where $0 \leq r < n$ and $q, r \in \mathbb{Z}$. Then

   $$x = g^k = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, ..., g^{n-1}\}.$$

   It follows that $\langle g \rangle = \{1, g, ..., g^{n-1}\}$.

□

Proposition 2.7 Let G be a group with element $g \in G$ where $o(g) = \infty$. Given $k \in \mathbb{Z}$, we have

1. $g^k = 1 \iff k = 0$
2. $g^k = g^m \iff k = m$
3. $\langle g \rangle = \{, ..., g^{-2}, g^{-1}, 1, g, g^2, ...\}$ where the g^i's are all distinct

PROOF

1. ($\Leftarrow$) $g^0 = 1$ by definition.

   ($\Rightarrow$) If $g^k = 1$ for some $k \neq 0$, then $g^{-k} = (g^k)^{-1} = 1$. So we can assume $k > 0$. However, this implies that $o(g)$ is finite: a contradiction. Thus, $k = 0$.

2. Note $g^k = g^m \iff g^{k-m} = 1$. By (1), $k - m = 0$, so $k = m$.
3. Follows from (2).

□

Proposition 2.8 Let G be a group where $g \in G$ and $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$, then

$$o(g^d) = \frac{n}{\gcd(n, d)}.$$

In particular, if $d|n$, then $\gcd(n, d) = d$ and $o(g^d) = \frac{n}{d}$.

Proof Let $n_1 = \frac{n}{\gcd(n,d)}$ and $d_1 = \frac{d}{\gcd(n,d)}$. By a result in MATH 135/145, $\gcd(n_1, d_1) = 1$. Note that

$$(g^d)^{n_1} = (g^d)^{\frac{n}{\gcd(n,d)}} = (g^n)^{\frac{d}{\gcd(n,d)}} = 1.$$

Thus, it remains to show that n_1 is the smallest such positive integer. Suppose $(g^d)^r = 1$ with $r \in \mathbb{N}$, then $g^{dr} = 1$. Thus, there exists $q \in \mathbb{Z}$ such that $dr = nq$ since $o(g) = n$ by Proposition 2.6. Dividing both sides by $\gcd(n, d)$:

$$\frac{dr}{\gcd(n, d)} = d_1 r = \frac{nq}{\gcd(n, d)} = n_1 q.$$

Since $n_1|d_1 r$ and $\gcd(n_1, d_1) = 1$, then $n_1|r$, meeaning $r = n_1 l$ for some $l \in \mathbb{Z}$. Since $r, n_1 \in \mathbb{N}$, it follows that $l \in \mathbb{N}$. Since $l \geq 1$, $r \geq n_1$, so n_1 is indeed the smallest positive integer giving $o(g^d) = n_1$. □

Subsection 2.4

Cyclic Groups

Recall that for a group G, if $G = \langle g \rangle$ for some $g \in G$, G is a cyclic group meaning for any $a, b \in G$, we have $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$. Since $ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba$, G is abelian.

Proposition 2.9 Every cyclic group is abelian.

Remark: the converse is not true; for example, K_4 is abelian but not cyclic.

Proposition 2.10 Every subgroup of a cyclic group is cyclic.

Proof Let $G = \langle g \rangle$ be a cyclic group and H be a subgroup of G. If $H = \{1\}$, then H is clearly cyclic. So, assume $H \neq \{1\}$ and let $g^k \in H$ where $k \in \mathbb{Z}$ and $k \neq 0$. Since H is a group, $g^{-k} \in H$ as well, so without the loss of generality, assume $k > 0$. Then, there exists a smallest positive integer m such that $g^m \in H$. We claim that g^m is a generator for H, that is, $\langle g^m \rangle = H$. Since $g^m \in H$, then $\langle g^m \rangle \subseteq H$. Week 3.2

To prove $H \subseteq \langle g^m \rangle$, let $h \in H$ be arbitrary. Write $h = g^k$ where $k \in \mathbb{Z}$. By division algorithm, we can write $k = qm + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Then

$$g^r = g^{k-mq} = g^k (g^m)^{-q} \in H.$$

Since $0 \leq r < m$ and m is the smallest positive integer such that $g^m \in H$, then $r = 0$. So, $m|k$ and $g^k \in \langle g^m \rangle$.

As $H = \langle g^m \rangle$, we have proven that H is cyclic, so we are done. □

Proposition 2.11 Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$. Then $G = \langle g^k \rangle$ if and only if $\gcd(n, k) = 1$.

PROOF By Proposition 2.8, we have

$$o(g^k) = \frac{n}{\gcd(n,k)} \iff o(g^k) = \frac{n}{1}.$$

□

Theorem 2.12 (Fundamental Theorem of Finite Cyclic Groups) Let $G = \langle g \rangle$ be a cyclic group, where $o(g) = n \in \mathbb{N}$.

1. If H is a subgroup of G, $H = \langle g^d \rangle$ for some $d|n$. It follows that $|H|||G|$.
2. Conversely, if $k|n$, then $\langle g^{n/k} \rangle$ is the unique subgroup of G of order k.

Remark: This shows there is a 1-1 correspondence between the set of positive divisors of n, and all subgroups of cyclic groups of order n.

PROOF

1. By Proposition 2.10, H is cyclic, say $H = \langle g^m \rangle$ for some $n \in \mathbb{N} \cup \{0\}$. Let $d = \gcd(m, n)$. First, we claim that $H = \langle g^d \rangle$: we will prove this.

   Since $d|m$, $m = dk$ for some $k \in \mathbb{Z}$. Then $g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle$. This proves $H \subseteq \langle g^d \rangle$. To prove $\langle g^d \rangle \subseteq H$, note that since $d = \gcd(m, n)$, there exist integers $x, y \in \mathbb{Z}$ where $d = mx + ny$ by a result in MATH 135/145. Then

   $$g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x 1^y \in \langle g^m \rangle = H$$

   Now that we have proven $H = \langle g^d \rangle$, note that since $d = \gcd(m, n)$, $d|n$. By Proposition 2.6 and 2.8,

   $$|H| = o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}.$$

   So, $|H|||G|$.

2. By Proposition 2.8, cyclic group $\langle g^{n/k} \rangle$ has order

   $$\frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

   To show uniqueness, let K be a subgroup of G with order k where $k|n$. By (1), let $K = \langle g^d \rangle$ where $d|n$. Then by Proposition 2.6 and 2.8,

   $$k = |K| = o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}.$$

   It follows that $d = \frac{n}{k}$ so $k = \langle g^{n/k} \rangle$.

□

SUBSECTION 2.5

Noncyclic Groups

Let X be a non-empty subset of group G and let

$$\langle X \rangle = \{x_1^{k_1} x_2^{k_2} ... x_m^{k_m} : x_i \in X, k_i \in \mathbb{Z}, m \geq 1\}$$

denote the set of all products of powers of (not necessarily distinct) elements of X. Note that if $x_1^{k_1}...x_m^{k_m} \in \langle X \rangle$ and $\tilde{x}_1^{r_1}...\tilde{x}_n^{r_n} \in \langle X \rangle$, then $x_1^{k_1}...x_m^{k_m}\tilde{x}_1^{r_1}...\tilde{x}_n^{r_n} \in \langle X \rangle$. Also, $x_1^0 \in \langle X \rangle$ and $(x_1^{k_1}...x_m^{k_m})^{-1} = x_m^{-k_m}...x_1^{-k_1} \in \langle X \rangle$. Hence, $\langle X \rangle$ is a subgroup of G containing X, called the subgroup of G generated by X.

Example $K_4 = \{1, a, b, c\}$ where $a^2 = b^2 = c^2 = 1$ and $ab = c$ (or $ac = b$ or $bc = a$) can be written

$$K_4 = \langle a, b : a^2 = 1 = b^2 \text{ and } ab = ba \rangle.$$

We can also replace a, b by a, c or b, c.

Example The symmetric group of degree 3, $S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $\sigma^3 = \epsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$. One can take $\sigma = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$. Thus,

$$S_3 = \langle \sigma, \tau : \sigma^3 = \epsilon = \tau^2, \sigma\tau = \tau\sigma^2 \rangle$$

We can also replace σ, τ with $\sigma, \tau\sigma$ or $\sigma, \tau\sigma^2$, etc.

Definition 2.8 (Dihedral Group) For $n \geq 2$, the dihedral group of order $2n$ is defined

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., ba^{n-1}\}$$

where $a^n = 1 = b^2$ and $aba = b$. Thus,

$$D_{2n} = \langle a, b : a^n = 1 = b^2, aba = b \rangle$$

Note that when $n = 2$ or $n = 3$, we have $D_4 \cong K_4$ and $D_6 \cong S_3$. Show this as an exercise.

Piazza Exercise: For $n \geq 3$, consider a regular n-gon and its group of symmetries. How does it relate to D_{2n}? Hint: consider all possible rotations and reflections.

End of Quiz 2 and Assignment 2 content.

Section 3

Normal Subgroups

Subsection 3.1

Homomorphisms and Isomorphisms

Week 3.3

Definition 3.1 Let G and H be groups. A mapping $\alpha : G \to H$ is a group homomorphism if $\alpha(a *_G b) = \alpha(a) *_H \alpha(b)$ for all $a, b \in G$.

To simplify notation, we often write $\alpha(ab) = \alpha(a)\alpha(b)$.

Example Cosnider the determinant map

$$\det : (GL_n(\mathbb{R}), \cdot) \to \mathbb{R}^*$$

given by $A \mapsto \det(A)$. Since $\det(AB) = \det(A)\det(B)$, det is a group homomorphism.

Proposition 3.1 Let $\alpha : G \to H$ be a group homomorphism. Then

1. $\alpha(1_G) = 1_H$
2. $\alpha(g^{-1}) = \alpha(g)^{-1}$ for all $g \in G$
3. $\alpha(g^k) = \alpha(g)^k$ for all $g \in G$

Proof Piazza Exercise. □

Definition 3.2 Let G and H be groups. Consider mapping $\alpha : G \to H$. If α is a homomorphism and α is bijective, we say α is an isomorphism. In this case, we say G and H are isomorphic and denote it as $G \cong H$.

Proposition 3.2 We have

1. The identity map $G \to G$ is an isomorphism
2. If $\sigma : G \to H$ is an isomorphism, then the inverse $\sigma^{-1} : H \to G$ is also an isomorphism
3. If $\sigma : G \to H$ and $\tau : H \to K$ are isomorphisms, then their composition $\tau\sigma : G \to K$ is also an isomorphism

Proof Piazza Exercise. □

We notice from Proposition 3.2 that $\cong$ is an equivalence relation.

Example Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$. We claim that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

Let $\sigma : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ be defined by $\sigma(r) = e^r$, the exponential function. Recall that exponentials map from $\mathbb{R}$ to $\mathbb{R}^+$ and is bijective. Also, for $r, s \in \mathbb{R}$ we have $\sigma(r + s) = e^{r+s} = e^r e^s = \sigma(r)\sigma(s)$. Thus, σ is a homomorphism and an isomorphism.

Example We claim that $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^*, \cdot)$. For the sake of contradiction, assume a $\tau : (\mathbb{Q}, +) \to (\mathbb{R}^*, \cdot)$ is an isomorphism. Then τ is onto. So, there exists $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Write $\tau(q/2) = a \in \mathbb{Q}$. Since τ is an isomorphism, we have

$$a^2 = \tau(q/2) + \tau(q/2) = \tau(q) = 2$$

which implies that $a = \sqrt{2}$ is rational. Clearly, this is not the case.

Subsection 3.2

Cosets and Lagrange Theorem

Definition 3.3 Let H be a subgroup of group G. If $a \in G$, we define $Ha = \{ha : h \in H\}$ as the right coset of H generated by a. Similarly, the left coset of H generated by a is $aH = \{ah : h \in H\}$.

Since $1 \in H$, $H1 = H = 1H$. This also implies that $a \in Ha$ and $a \in aH$. Note that in general, Ha and aH are not subgroups of G and $Ha \neq aH$. However, if G is abelian, then $aH = Ha$.

Example Let $K_4 = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ab = ba$. Let $H = \{1, a\}$ which we can see is a subgroup of K_4. Note that since K_4 is abelian, $gH = Hg$ for any $g \in K_4$. Then the right and left cosets of H are $H1 = \{1, a\} = Ha$ and $Hb = \{b, ab\} = Hab$. Thus, exactly 2 cosets of H are in K_4.

Example Consider $S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ with $\sigma^3 = \epsilon = \tau^2$ and $\sigma\tau\sigma = \tau$. Let $H = \{\epsilon, \tau\}$ be a subgroup of S_3. Since $\sigma\tau = \tau\sigma^{-1} = \tau\sigma^2$, the right cosets of H are $H\epsilon\{\epsilon, \tau\} = H\tau$, $H\sigma = \{\sigma, \tau, \sigma\} = H\tau\sigma$, and $H\sigma^2 = \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2$. Also, the left cosets of H are $\epsilon H = \{\epsilon, \tau\} = \tau H$, $\sigma H = \{\sigma, \tau\sigma^2\} = \tau\sigma^2 H$, and $\sigma^2 H = \{\sigma^2, \tau\sigma\} = \tau\sigma H$. Note that $H\sigma \neq \sigma H$ and $H\sigma^2 \neq \sigma^2 H$.

Proposition 3.3 Let H be a subgroup of group G where $a, b \in G$.

1. $Ha = Hb$ iff $ab^{-1} \in H$. In particular, $Ha = H$ iff $a \in H$ by taking $b = 1$
2. If $a \in Hb$, $Ha = Hb$
3. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Thus, distinct right cosets of H form a partition of G.

Proof

1. ($\Longrightarrow$) If $Ha = Hb$, $a = 1a \in Ha = Hb$. So $a = hb$ for some $b \in H$, meaning $ab^{-1} = h \in H$.

   ($\Longleftarrow$) Suppose $ab^{-1} \in H$. Then, for all $h \in H$, $ha = ha(b^{-1}b) = h(ab^{-1})b \in Hb$. So, $Ha \subseteq Hb$. Note if $ab^{-1} \in H$, since H is a subgroup, then $(ab^{-1})^{-1} = ba^{-1} \in H$. So, for all $h \in H$, $hb = hb(a^{-1}a) = h(ba^{-1})a \in Ha$. We conclude that $Ha = Hb$.
2. If $a \in Hb$, then $ab^{-1} \in H$. Then, by (1), $Ha = Hb$.
3. We have two cases. If $Ha \cap Hb = \emptyset$, we are done. So, assume $Ha \cap Hb \neq \emptyset$. There exists an element $x \in Ha \cap Hb$. Since $x \in Ha$, by (2) $Hx = Ha$. Since $x \in Hb$, by (2) $Hx = Hb$. So we conclude $Ha = Hb$.

□

Remark: the analogous of Proposition 3.3 also holds for left cosets. In particular, for (1) we have $aH = bH$ iff $b^{-1}a \in H$. Week 4.1

Definition 3.4 (Index) Let G be a group and H be a subgroup of G. We define the index $[G : H]$ to be the number of right (or left) cosets of H in G.

Theorem 3.4 (Lagrange's Theorem) Let H be a subgroup of a finite group G. We have $|H|||G|$ and

$$[G : H] = \frac{|G|}{|H|}.$$

Proof Write $k = [G : H]$ and let $Ha_1, ..., Ha_k$ be the distinct right cosets of H in G. By Proposition 3.3, we can write G as a disjoint union

$$G = Ha_1 \cup ... \cup Ha_k.$$

Note that $Ha_i = \{ha_i : h \in H\}$ so $|H| = |Ha_i|$ for each $1 \leq i \leq k$. Then

$$|G| = |Ha_1| + ... + |Ha_k| = |H| + ... + |H| = k|H|.$$

It follows that $|H|||G|$ and $k = \frac{|G|}{|H|}$. □

Corollary 3.5

1. If G is a finite group and $g \in G$, then $o(g)||G|$
2. If G is a finite group with $|G| = n$, then for all $g \in G$, we have $g^n = 1$

Proof

1. Take $H = \langle g \rangle$ in Theorem 3.4. Note that $|H| = o(g)$, which gives the result.
2. Let $o(g) = m$. By (1), $m|n$. Thus,

$$g^n = (g^m)^{n/m} = 1^{n/m} = 1.$$

□

Example For $n \in \mathbb{N}$ with $n \geq 2$, let $\mathbb{Z}_n^*$ be the set of multiplicative invertible elements in $\mathbb{Z}_n$. Let the Euler's φ function denote the order of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\{[k] \in \mathbb{Z}_m : k \in \{0, 1, ..., n-1\}, \gcd(k, n) = 1\}|.$$

As direct consequence of Corollary 3.5, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. This is Euler's Theorem.

If $n = p$, a prime number, Euler's Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's Little Theorem.

We recall by constructing their Cayley table that we can show for a group G, $G \cong C_2$ if $|G| = 2$, and $G \cong C_3$ if $|G| = 3$. We now can see a more general result:

Corollary 3.6 If G is a group with $|G| = p$ where p is a prime, then $G \cong C_p$, the cyclic group of order p.

Proof Let $g \in G$ where $g \neq 1$. By Corollary 3.5, $o(g)|p$. Since $g \neq 1$, and p is prime, then $o(g) = p$. □

Corollary 3.7 Let H and K be finite subgroups of group G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof By Proposition 2.1, $H \cap K$ is a subgroup of H and K. By Lagrange's Theorem, $|H \cap K|||H|$ and $|H \cap K|||K|$. It follows that $|H \cap K||\gcd(|H|, |K|)$. Since $\gcd(||H|, |K|) = 1$ by assumption, $|H \cap K| = 1$. Since $1 \in H, K$, then $H \cap K = \{1\}$. □

Subsection 3.3

Normal Subgroups

Let H be a subgroup of group G where $g \in G$. In general, we know $Hg \neq gH$. However, we can look at the special case where $Hg = gH$.

Definition 3.5 (Normal Subgroup) Let H be a subgroup of group G. If $gH = Hg$ for all $g \in G$, we say H is normal in G, denoted $H \triangleleft G$.

Warning: note that $Hg = gH$ does not imply $gh = hg$ where $h \in H$.

Example We have $\{1\} \triangleleft G$ and $G \triangleleft G$.

Example The center $Z(G)$ of G, $Z(G) = \{z \in G : zg = gz, \forall g \in G\}$ is an abelian subgroup of G. By its definition, $Z(G) \triangleleft G$. So, every subgroup of $Z(G)$ is normal in G.

Example If G is an abelian group, every subgroup of G is normal in G. However, the converse is false. See the quarternion group in Assignment 3.

Proposition 3.8 (Normality Test) Let H be a subgroup of group G. The following are equivalent:

1. $H \triangleleft G$
2. $gHg^{-1} \subseteq H$ for all $g \in G$
3. $gHg^{-1} = H$ for all $g \in G$

Proof (1) $\implies$ (2). Let $x \in gHg^{-1}$, so $x = ghg^{-1}$ for some $h \in H$. By (1), $gh \in gH = Hg$, say $gh = h_1 g$ for some $h_1 \in H$. Then $x = ghg^{-1} = h_1 gg^{-1} = h_1 \in H$.

(2) $\implies$ (3). If $g \in H$, by (2) $gHg^{-1} \subseteq H$. Taking g^{-1} in place of G in (2), $g^{-1}Hg \subseteq H$. This implies that $H \subseteq gHg^{-1}$. It follows that $gHg^{-1} = H$.

(3) $\implies$ (1). If $gHg^{-1} = H$, then $gH = Hg$, which means $H \triangleleft G$ by definition. □

Example Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$. For $A \in G$ and $B \in H$, Week 4.2

$$\det\left(ABA^{-1}\right) = \det(A)\det(B)\frac{1}{\det(A)} = \det(B) = 1.$$

So, $ABA^{-1} \in H$ implies $AHA^{-1} \subseteq H$ for all $A \in G$. By the Normality Test, $H \triangleleft G$.

Proposition 3.9 If H is a subgroup of group G, and $[G : H] = 2$, then $H \triangleleft G$.

Proof Let $g \in G$. If $g \in H$, then $H = Hg = gH$ by Proposition 3.3. If $g \notin H$, then since $[G : H] = 2$, $G = H \cup Hg$, a disjoint union. Thus $Hg = G \backslash H$. Similarly, $gH = G \backslash H$. So, $Hg = gH$ in either case. By definition $H \triangleleft G$. □

Example Let A_n be the alternating group contained in S_n. Since $[S_n : A_n] = 2$, then $A_n \triangleleft S_n$ by Proposition 3.9.

Example Let $D_{2n} = \langle a, b : a^n = 1 = b^2, aba = b\rangle$ be the dihedral group of order $2n$. Since $[D_{2n} : \langle a\rangle] = 2$, then $\langle a\rangle \triangleleft D_{2n}$ by Proposition 3.9.

Let H, K be subgroups of group G. The intersection $H \cap K$ is what we call the "largest" subgroup of G contained in both H and K.

There is also a "smallest" subgroup containing both H and K: this is $H \cup K$. Recall from Assignment 2 that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$. Hence, this is the case.

A more useful intersection turns out to be the product of H and K, defined

$$HK = \{hk : h \in H, k \in K\}.$$

There is still cases where this is not a group.

Exercise: Find an example when HK is not a subgroup.

Lemma 3.10 Let H and K be subgroups of group G. The following are equivalent:

1. HK is a subgroup of G
2. $HK = KH$
3. KH is a subgroup of G

Proof Note that we only need to prove (1) $\iff$ (2), then (2) $\iff$ (3) follows by interchanging H and K.

(2) $\implies$ (1). We have $1 = 1 \cdot 1 \in HK$. If $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Also, if $hk, h_1k_1 \in HK$, then $kh_1 \in KH = HK$ too, say $kh_1 = h_2k_2$. Then

$$hkh_1k_1 = hh_2k_2k_1 = (hh_2)(k_2k_1) \in HK$$

and we have satisfied all 3 requirements of the subgroup test.

(1) $\implies$ (2). Let $kh \in KH$. Since H, K are subgroups of G, $h^{-1} \in H$ and $k^{-1} \in K$. Since HK is also a subgroup of G, $kh = (h^{-1}k^{-1})^{-1} \in HK$. So $KH \subseteq HK$. On the other hand, if $hk \in HK$, since HK is a subgroup of G, $k^{-1}h^{-1} = (hk)^{-1} \in HK$, say $k^{-1}h^{-1} = h_1k_1$. Then $hk = k_1^{-1}h_1^{-1} \in KH$. So $HK \subseteq KH$. Since both inclusions are shown, $KH = HK$. □

Proposition 3.11 Let H and K be subgroups of group G.

1. If $H \triangleleft G$ or $K \triangleleft G$, then $HK = KH$ is a subgroup of G
2. If $H \triangleleft G$ and $K \triangleleft G$, $HK \triangleleft G$

Proof

1. Suppose $H \triangleleft G$. Then
$$HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = kH.$$
By Lemma 3.10, $HK = KH$ is a subgroup of G.
2. If $g \in G$ and $hk \in HK$, since $H \triangleleft G$ and $K \triangleleft G$,
$$g^{-1}hkg = g^{-1}hgg^{-1}kg = (g^{-1}hg)(g^{-1}kg) \in HK$$
So $HK \triangleleft G$.

□

Exercise: Find an example where $HK = KH$ is a subgroup of G but H and K are not normal in G.

Definition 3.6 (Normalizer) Let H be a subgroup of G. The normalizer of H, denoted by $N_G(H)$, is defined
$$N_G(H) = \{g \in G : gH = Hg\}.$$

We see $H \triangleleft G$ iff $N_G(H) = G$. Now, note that in the proof of Proposition 3.11, we only need $Hk = kH$ for all $k \in K$ (i.e. $k \in N_G(H)$).

Corollary 3.12 Let H and K be subgroups of group G. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$), then $HK = KH$ is also a subgroup of G.

Theorem 3.13 If $H \triangleleft G$ and $K \triangleleft G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

Proof

We first prove the following claim: If $H \triangleleft G$ and $K \triangleleft G$ satisfy $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. Week 4.3

Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $kh^{-1}k \in kHk^{-1} = H$. Thus, $x \in H$. Similarly, $hkh^{-1} \in hKh^{-1} = K$, so $x \in K$. Overall, $x = 1$ by assumption. Then
$$1 = hkh^{-1}k^{-1} \implies kh = hk.$$

We have finished proving the claim. Next, since $H \triangleleft G$, by Proposition 3.11 HK is a subgroup of G. Define $\sigma : H \times K \to HK$ by $\sigma((h,k)) = hk$ for all $h \in H$ and $k \in K$. The second claim we will prove is that σ is an isomorphism.

First, let (h,k) and $(h_1,k_1) \in H \times K$. By the previous claim, $h_1k = kh_1$. Then,
$$\begin{aligned}\sigma((h,k)\cdot(h_1,k_1)) &= \sigma((hh_1,kk_1))\\ &= hh_1kk_1\\ &= hkh_1k_1\\ &= \sigma((h,k))\sigma((h_1,k_1))\end{aligned}$$

So, σ is a homomorphism. By the definition of HK, σ is onto. So, all that is left is to show σ is one-to-one. Let $\sigma((h,k)) = \sigma((h_1,k_1))$. Then
$$hk = h_1k_1 \implies h_1^{-1}h = k_1k^{-1} \implies h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}.$$

So $h = h_1$ and $k = k_1$. Since σ is a bijection, it follows that σ is an isomorphism and $HK \cong H \times K$. □

Corollary 3.14 Let G be a finite group and let $H \triangleleft G$ and $K \triangleleft G$ with $H \cap K = \{1\}$ and $|H||K| = |G|$. Then $G \cong H \times K$.

Example Let $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Let G be a cyclic group of order mn. Write $G = \langle a \rangle$ where $o(a) = mn$. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Thus $|H| = o(a^n) = m$ and $|K| = o(a^m) = n$. It follows that $|H||K| = mn = |G|$. Since $\gcd(m, n) = 1$, by Corollary 3.7 $H \cap K = \{1\}$. Also, since G is cyclic, G is abelian and $H \triangleleft G$ and $K \triangleleft G$. So, by Theorem 3.14, $G \cong H \times K$:

$$C_{mn} \cong C_m \times C_n.$$

Hence to consider finite cyclic groups, it suffices to consider cyclic groups of prime power order.

End of Quiz 3 and Assignment 3 content

Section 4

Isomorphism Theorems

Subsection 4.1

Quotient Groups

Let G be a group and K be a subgroup of G. A question we have is whether we can make the right cosets of K $\{Ka : a \in G\}$ into a group.

A natural way to define multiplication on this set is $KaKb = Kab$ for all $a, b \in G$.

However, note that we can have $Ka = Ka_1$ and $Kb = Kb_1$ where $a \neq a_1$ and $b \neq b_1$. Thus, in order for this multiplication to make sense, a necessary condition is that

$$Ka = Ka_1 \text{ and } Kb = Kb_1 \implies Kab = Ka_1b_1.$$

In this case, we say that the multiplication $KaKb = Kab$ is well defined.

Lemma 4.1 Let K be a subgroup of group G. The following are equivalent:

1. $K \triangleleft G$
2. For $a, b \in G$, $KaKb = Kab$ is well defined

Proof (1) $\implies$ (2). Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus, $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To get $Kab = Ka_1b_1$, it suffices to show that $ab(a_1b_1)^{-1} \in K$. Since $K \triangleleft G$, $aKa^{-1} \subseteq K$. Thus, $ab(a_1b_1)^{-1} = ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a^{-1} \in K$. Since $aa_1^{-1} \in K$ too, then

$$a(bb_1^{-1})a^{-1}(aa_1^{-1}) \in K$$

It follows that $Kab = Ka_1b_1$.

(2) $\implies$ (1). If $a \in G$, to show $K \triangleleft G$, it suffices to show that $aka^{-1} \in K$ for all $k \in K$. Since $Ka = Ka$ and $Kk = K1$, by (2) $Kak = Ka1$. It follows that $aka^{-1} \in K$, so $K \triangleleft G$. □

Proposition 4.2 Let $K \triangleleft G$ and write $G/K = \{Ka : a \in G\}$ for the set of all cosets of K.

1. G/K is a group under the operation $Kab = KaKb$
2. The mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is an onto homomorphism.
3. If $[G : K]$ is finite, $|G/K| = [G : K]$. In particular, $|G/K| = \frac{|G|}{|K|}$.

Proof

1. By Lemma 4.1, the operation is well defined and G/K is closed under operation. The identity of G/K is $K = K1$. Also, $KaKa^{-1} = K1 = Ka^{-1}Ka$. Finally, $Ka(KbKc) = (KaKb)Kc$ by the associativity of G. Thus G/K is a group.
2. φ is clearly onto. Also, for $a, b \in G$ we have $\varphi(a)\varphi(b) = KaKb = Kab = \varphi(ab)$.
3. If $[G : K]$ is finite, by definition of $[G : K]$ we have $[G : K] = |G/K|$. Also, if $|G|$ is finite, by Lagrange's Theorem, $|G/K| = \frac{|G|}{|K|}$.

□

Definition 4.1 (Quotient Group) Let $K \triangleleft G$ where K is a subgroup of group G. The group G/K of all cosets of K in G is called the quotient group of G by K. Also, the map $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is called the coset map.

Week 5.1

Exercise: Let

$$D_{10} = \langle a, b : a^5 = 1 = b^2, aba = b \rangle$$

be the Dihedral group of order 10. List all normal subgroups K of D_{10} and all quotient groups D_{10}/K.

Subsection 4.2

Isomorphism Theorems

Definition 4.2 (Kernel and Image) Let $\alpha : G \to H$ be a group homomorphism. The kernel of α is defined

$$\ker \alpha = \{g \in G : \alpha(g) = 1\} \subseteq G$$

and the image of α is defined

$$\text{im}\alpha = \alpha(G) = \{\alpha(g) : g \in G\} \subseteq H.$$

Proposition 4.3 Let $\alpha : G \to H$ be a group homomorphism.

1. $\text{im}\alpha$ is a subgroup of H
2. $\ker \alpha$ is a normal subgroup of G

Proof

1. Note that $1_H = \alpha(1_G) \in \alpha(G)$. Also, for $h_1 = \alpha(g_1)$ and $h_2 = \alpha(g_2)$ in $\alpha(G)$, we have $h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G)$. Also, by Proposition 3.1, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$. By the Subgroup Test, we conclude $\alpha(G)$ is a subgroup of H.
2. Note that $\alpha(1_G) = 1_h$. Also, if $k_1, k_2 \in \ker \alpha$, $\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1$. And $\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1$. So $\ker \alpha$ is a subgroup of G. Let $g \in G$ and $k \in \ker \alpha$. Then $\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)1\alpha(g^{-1}) = 1$. So, $g(\ker \alpha)g^{-1} \subseteq \ker \alpha$. By the Normality Test, $\ker \alpha \triangleleft G$.

□

Example Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ defined $A \mapsto \det(A)$. Then $\ker(\det) = SL_n(\mathbb{R})$, the special linear group. Thus $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$.

Example Define the sign of a permutation $\sigma \in S_n$ by

$$\text{sgn}(\alpha) = \begin{cases} 1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases}$$

Then, the sign mapping $\text{sgn} : S_n \to \{\pm 1\}$ defined $\sigma \mapsto \text{sgn}(\sigma)$ is a homomorphism. Also, $\ker(\text{sgn}) = A_n$, the alternating group. So $A_n \triangleleft S_n$.

Theorem 4.4 (1st Isomorphism Theorem) Let $\alpha : G \to H$ be a group homomorphism. Then we have

$$G/\ker \alpha \cong \text{im}\alpha.$$

Proof Let $K = \ker\alpha$. Since $K \triangleleft G$, G/K is a group. Define the group map $\bar{\alpha} : G/K \to \text{im}\alpha$ by

$$\bar{\alpha}(Kg) = \alpha(g).$$

Note that for $g, g_1 \in G$,

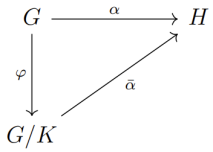
$$Kg = Kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg^{-1}) = 1 \iff \alpha(g) = \alpha(g_1).$$

So, $\bar{\alpha}$ is well defined, and one-to-one. It is clear by construction that $\bar{\alpha}$ is onto. It remains to show that $\bar{\alpha}$ is a group homomorphism. For $g, h \in G$,

$$\bar{\alpha}(KgKh) = \bar{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h) = \bar{\alpha}(Kg)\bar{\alpha}(Kh).$$

So $\bar{\alpha}$ is a group isomorphism, and $G/K \cong \text{im}\alpha$. □

Let $\alpha : G \to H$ be a group homomorphism and $K = \ker\alpha$. Let $\varphi : G \to G/K$ be the coset map and let $\bar{\alpha}$ be defined as in the proof of Theorem 4.4. Then,



Note for $g \in G$, we have $\bar{\alpha}\varphi(g) = \bar{\alpha}(Kg) = \alpha(g)$. Thus $\alpha = \bar{\alpha}\varphi$. On the other hand, if we have $\alpha = \bar{\alpha}\varphi$ then the action of $\bar{\alpha}$ is determined by α and φ as

$$\bar{\alpha}(Kg) = \bar{\alpha}(\varphi(g)) = \bar{\alpha}\varphi(g) = \alpha(g).$$

Proposition 4.5 Let $\alpha : G \to H$ be a group homomorphism and $K = \ker\alpha$. Then α factors uniquely as $\alpha = \bar{\alpha}\varphi$ where $\varphi : G \to G/K$ is the coset map and $\bar{\alpha} : G/K \to H$ is defined by $\bar{\alpha}(Kg) = \alpha(g)$. Note that φ is onto and $\bar{\alpha}$ is one-to-one.

Example We have seen that $\mathbb{Z} = \langle \pm 1 \rangle$ and $\mathbb{Z}_n = \langle [1] \rangle$ for some $n \in \mathbb{N}$. Let $G = \langle g \rangle$ be a cyclic group. Consider the map $\alpha : (\mathbb{Z}, +) \to G$ defined $\alpha(k) = g^k$ for all $k \in \mathbb{Z}$, which is a group homomorphism. By the definition of $\langle g \rangle$, α is onto. Note that $\ker\alpha = \{k \in \mathbb{Z} : g^k = 1$. There are two cases:

1. If $o(g) = \infty$, $\ker\alpha = \{0\}$. By the first isomorphism theorem,
$$G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$$
2. If $o(g) = n \in \mathbb{N}$, by Proposition 2.6 $\ker\alpha = n\mathbb{Z}$. By the first isomorphism theorem,
$$G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

By (1) and (2), we can conclude that if G is a cyclic group, $G \cong \mathbb{Z}$ or $C \cong \mathbb{Z}_n$.

Theorem 4.6 (2nd Isomorphism Theorem) Let H and K be subgroups of G with $K \triangleleft G$. Then, HK is a subgroup of G, $K \triangleleft HK$, $H \cap K \triangleleft H$, and

$$HK/K \cong H/(H \cap K).$$

Week 5.2

Proof Since $K \triangleleft G$, by Proposition 3.11 $HK = KH$ is a subgroup of G. Then, by the definition of normal subgroups, $K \triangleleft HK$. Consider the map $\alpha : H \to HK/K$ defined $\alpha(h) = Kh$. We claim α is an homomorphism (prove this as an exercise).

Also, if $x \in HK = KH$, say $x = kh$, then $Kx = K(kh) = Kh = \alpha(h)$, so α is onto. Finally, by Proposition 3.3,

$$\ker \alpha = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = H \cap K.$$

By the 1st isomorphism theorem, $H/(H \cap K) \cong HK/K$. □

Theorem 4.7 (3rd Isomorphism Theorem) Let $K \subseteq H \subseteq G$ be groups where $K \triangleleft G$ and $H \triangleleft G$. Then $H/K \triangleleft G$ and

$$(G/K)/(H/K) \cong G/H.$$

Proof Let $\alpha : G/K \to G/H$ be defined $\alpha(Kg) = Hg$ for all $g \in G$. Note that if $Kg = Kg_1$ for $g, g_1 \in G$, $gg_1^{-1} \in K \subseteq H$. Thus, $Hg = Hg_1$ and α is well defined. Clearly, α is onto. Note that

$$\ker \alpha = \{Kg : Hg = H\} = \{Kg : g \in G\} = H/K.$$

By the 1st isomorphism theorem, $(G/K)/(H/K) \cong G/H$. □

End of Quiz 4 and Assignment 4 content

Section 5

Group Actions

Subsection 5.1

Cayley's Theorem

Theorem 5.1 (Cayley's Theorem) If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof Let $G = \{g_1, ..., g_n\}$ and S_G be the permutation group of G. By identifying g_i with i for $i = 1, ..., n$, we see that $S_G \cong S_n$. So, to prove this theorem, it sufficies to find a one-to-one homomorphism $\sigma : G \to S_G$.

For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. Note that if $ag = ag_1$ for $g, g_1 \in G$, $g = g_1$ and $a(a^{-1}g) = g$. So, μ_a is a bijection and $\mu_a \in S_G$. Define $\sigma : G \to S_G$ by $\sigma(a) = \mu_a$. For $a, b \in G$ we have $\mu_a\mu_b = \mu_{ab}$ so σ is a homomorphism. Also, if $\mu_a = \mu_b$,

$$a = \mu_a(1) = \mu_b(1) = b$$

so σ is a one-to-one homomorphism. By the 1st isomorphism theorem, $G \cong \text{im}\sigma$, a subgroup of $S_G \cong S_n$. □

Example Let H be a subgroup of group G with $[G : H] = m < \infty$. Let $X = \{g_1H, ..., g_mH\}$ be the set of all distinct left cosets of H in G. For $a \in G$, define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$ for all $gH \in X$. Note that $agH = ag_1H$ implies $gH = g_1H$ and $a(a^{-1}gH) = gH$, hence λ_a is a bijection and $\lambda_a \in S_X$, the permutation group of X.

Consider the map $\tau : G \to S_X$ defined $\tau(a) = \lambda a$. For $a, b \in G$, $\lambda_{ab} = \lambda_a\lambda_b$ so τ is a homomorphism. Note that if $a \in \ker\tau$, then λ_a is the identity permutation. In particular, $aH = \lambda_a(H) = H$ meaing $a \in H$, so $\ker\tau \subseteq H$.

Theorem 5.2 (Extended Cayley Theorem) Let H be a subgroup of G with $[G : H] = m < \infty$. If G has no normal subgroups contained in H except $\{1\}$, then G is isomorphic to a subgroup of S_m.

Proof Let X be the set of all distinct left cosets of H in G. We have $|X| = m$ and $S_X \cong S_m$. We have seen from the above example that there exists a group homomorphism $\tau : G \to S_X$ with $K = \ker\tau \subseteq H$. By the 1st isomorphism theorem, we have $G/K \cong \text{im}\tau$. Since $K \subseteq H$, and $K \triangleleft G$ by Proposition 4.3, then $K = \{1\}$ by assumption. It follows that $G \cong \text{im}\tau$, a subgroup of $S_X \cong S_m$. □

Corollary 5.3 Let G be a finite group and p be the smallest prime dividing $|G|$. If H is a subgroup of G with $[G : H] = p$, then $H \triangleleft G$. Week 5.3

Proof Let X be the set of all distinct left cosets of H in G. We have $|X| = p$ and $S_X \cong S_p$. Let $\tau : G \to S_X$ be the group homomorphism defined in the proof of Theorem 5.2 where $K = \ker\tau \subseteq H$. By the first isomorphism theorem, $G/K \cong \text{im}\tau \subseteq S_p$. So, G/K is isomorphic to a subgroup of S_p. By Lagrange's Theorem, $|G/k||p!$ since $|S_p| = p!$.

Also, since $K \subseteq H$, if $[H : K] = k$, then

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K] = pk$$

So, $pk|p!$ and so $k|(p-1)!$. Since $k||H|$ which divides $|G|$ and p is the smallest prime dividing $|G|$, we see that we must have $k = 1$, implying $K = H$. So, $H \triangleleft G$.

□

Note that this corollary is a generalization of Proposition 3.9 where $p = 2$.

Subsection 5.2

Group Actions

Definition 5.1 (Group Action) Let G be a group and X be a non-empty set. A (left) group action of G on X is a mapping $G \times X \to X$ denoted by $(a, x) \mapsto a \cdot x$ such that

1. $1 \cdot x = x$ for all $x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x$ for all $a, b \in G$ and $x \in X$

In this case, we say that G acts on X.

Remark: Let G be a group acting on set $X \neq \emptyset$. For $a, b \in G$ and $x, y \in X$, by (1) and (2) above we have

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y.$$

In particular, $a \cdot x = a \cdot y$ if and only if $x = y$.

Example If G is a group, let G act on itself ($X = G$) by conjugation:

$$a \cdot x = axa^{-1}$$

for all $a, x \in G$. In other words, we have a mapping $G \times G \to G$ with $(a, x) \mapsto axa^{-1}$. Note that $1 \cdot x = 1x1^{-1} = x$ and

$$a \cdot (b \cdot x) = a \cdot (bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab) \cdot x.$$

Remark: For $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. Then, one can show (in Assignment 5) that

1. $\sigma_a \in S_X$, the permutation group of X
2. The function $\theta : G \to S_X$ defined by $\theta(a) = \sigma_a$ is a group homomorphism with

$$\ker\theta = \{a \in G : a \cdot x = x, \forall x \in X\}$$

Note that the group homomorphism $\theta : G \to S_X$ gives an equivalent definition of a group action of G on X. If $X = G$ and $|G| = n$ and $\ker\theta = \{1\}$ (called a faithful group action), the map $\theta : G \to S_n$ shows that G is isomorphic to a subgroup of S_n, which is Cayley's Theorem.

Definition 5.2 (Orbit and Stabilizer) Let G be a group acting on a set $X \neq \emptyset$ and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : g \in G\} \subseteq X$$

the orbit of x, and

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the stabilizer of x.

Proposition 5.4 Let G be a group acting on a set $X \neq \emptyset$ and $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizers of x respectively. Then

1. $S(x)$ is a subgroup of G
2. There exists a bijection from $G \cdot x$ to $\{gS(x) : g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$.

Proof

1. Since $1 \cdot x = x$, $1 \in S(x)$. Also, if $g, h \in S(x)$, then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ so $gh \in S(x)$. Lastly, $g^{-1}x = g^{-1}(g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x$ so $g^{-1} \in S(x)$, and so $S(x)$ is a subgroup by the Subgroup Test.
2. Consider the map $\varphi : G \cdot x \to \{gS(x) : g \in G\}$ defined $\varphi(g \cdot x) = gS(x)$. Note that Week 6.1

$$g \cdot x = h \cdot x \iff h^{-1}g \in S(x) \iff gS(x) = hS(x).$$

Thus, φ is well defined and one-to-one. Since φ is clearly onto, it follows that φ is a bijection.

□

Theorem 5.5 (Orbit Decomposition Theorem) Let G be a group acting on a finite set $X \neq \emptyset$. Let

$$X_f = \{x \in X : a \cdot x = x \, \forall a \in G\}.$$

Note that $x \in X_f \iff |G \cdot x| = 1$. Let

$$G \cdot x_1, G \cdot x_2, ..., G \cdot x_n$$

denote the distinct nonsingleton orbit ($|G \cdot x_i| > 1$). Then

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)].$$

Proof Note that for $a, b \in G$ and $x, y \in X$,

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y \iff y \in G \cdot x \iff G \cdot x = G \cdot y.$$

Thus, 2 orbits are either disjoint or the same. It follows that the orbits form a disjoint union of X. Since $x \in X_f \iff |G \cdot x| = 1$, the set $X \backslash X_f$ contains all nonsingleton orbits which are disjoint. Thus, by Proposition 5.4,

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)].$$

□

Let G be a group acting on itself by conjugation: $g \cdot x = gxg^{-1}$. Then

$$G_f = \{x \in G : gxg^{-1} = x \, \forall g \in G\} = \{x \in G : g \cdot x = x \cdot g \, \forall g \in G\} = Z(G).$$

Also, for $x \in G$,

$$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

This set is called the centralizer of x and is denoted $S(x) = C_G(x)$. Finally, in this case, the orbit

$$G \cdot x = \{gxg^{-1} : g \in G\}$$

is called the conjugacy class of x.

Corollary 5.6 (Class Equation) Let G be a finite group and

$$\{gx_1g^{-1} : g \in G\}, ..., \{gx_ng^{-1} : g \in G\}$$

denote the distinct nonsingleton conjugacy classes in G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)].$$

Lemma 5.7 Let p be a prime and $m \in \mathbb{N}$. Let G be a group of order p^m acting on a finite set $X \neq \emptyset$. Let X_f be defined as in Theorem 5.5. Then,

$$|X| \equiv |X_f| \pmod{p}.$$

Proof By Theorem 5.5, we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

where $[G : S(x_i)] > 1$ for all i. Since $[G : S(x_i)] > 1$, we have $p|[G : S(x_i)]$ by Lagrange's Theorem. It follows that

$$|X| \equiv |X_f| \pmod{p}.$$

□

Theorem 5.8 (Cauchy's Theorem) Let p be a prime and G be a finite group. If $p||G|$, then G contains an element of order p.

Proof (By J. McKay). Define

$$X = \{(a_1, ..., a_p) : a_i \in G, a_1a_2...a_p = 1\}.$$

Since a_p is uniquely determined by $a_1, ..., a_{p-1}$, if $|G| = n$, we have $|X| = n^{p-1}$. Since $p|n$, we have $|X| \equiv 0 \pmod{p}$. Let group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by cycling: for $k \in \mathbb{Z}_p$,

$$k \cdot (a_1, ..., a_p) = (a_{k+1}, ..., a_1, ..., a_k).$$

One can verify that this action is well defined (exercise). Let X_f be defined as in

Theorem 5.5. Then,

$$(a_1, ..., a_p) \in X_f \iff a_1 a_1 = a_2 = ... = a_p.$$

Clearly, $(1, ..., 1) \in X_f$, so $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, by Lemma 5.7,

$$|X_f| \equiv |X| \equiv 0 \pmod{p}.$$

Since $|X_f| \equiv 0 \pmod{p}$ and $|X_f| \geq 1$, it follows that $|X_f| \geq p$, so an element $(a, ..., a) \in X_f$ exists where $a^p = 1$. Since p is a prime, and $a \neq 1$, the order of a is p. □

Section 6

Sylow Theorems

Subsection 6.1

p-Groups

Definition 6.1 (p-Group) Let p be prime. A group in which every element has order of a non-negative power of p is called a p-group.

Week 6.2

As a direct corollary of Cauchy's theorem, we have

Corollary 6.1 A finite group G is a p-group iff $|G|$ is a power of p.

Lemma 6.2 The center $Z(G)$ of a nontrivial finite p-group contains more than one element.

Proof The class equation of G states that

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)].$$

Since G is a p-group, then by Corollary 6.1, $p||G|$. By Lemma 5.7, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$. Since $1 \in Z(G)$ and $|Z(G)| \geq 1$, then $|Z(G)| \geq p$. □

Lemma 6.3 If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof Recall that $N_G(H) = \{g \in G : gHg^{-1} = H\}$ is the normalizer of H in G. Let X be the set of all left cosets of H in G. So, $|X| = [G : H]$. Let H act on X by left multiplication. Then, for $x \in G$,

$$\begin{aligned} xH \in X_f &\iff hxH = xH \ \forall h \in H \\ &\iff x^{-1}hxH = H \ \forall h \in H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus, $|X_f|$ is the number of cosets xH with $x \in N_G(H)$, so $|X_f| = [N_G(H) : H]$. The result follows by Lemma 5.7. □

Corollary 6.4 Let H be a p-subgroup of a finite group G. If $p|[G : H]$, then $p|[N_G(H) : H]$ and $N_G(H) \neq H$.

Proof Since $p|[G : H]$, by Lemma 6.3 we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}.$$

Since $p|[N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. So, $N_G(H) \neq H$. □

Subsection 6.2
Sylow's Three Theorems

Week 6.3

Theorem 6.5 (1st Sylow Theorem) Let G be a group of order $p^n m$ where p is prime, $n \geq 1$, and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Proof We will prove this by induction on i. For $i = 1$, since $p||G|$, G contains an element of order p by Cauchy's theorem. If $a \in G$ where $o(a) = p$, then $|\langle a \rangle| = p$ is a subgroup of order p.

For the inductive step, assume for some $1 \leq i < n$ the statement holds: H is a subgroup of G of order p^i.

Then, $p|[G : H]$. By Corollary 6.4, $p|[N_G(H) : H]$ and $[N_G(H) : H] \geq p$. By Cauchy's theorem, $N_G(H)/H$ contains an element of order p. Such a group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \triangleleft N_G(H)$, we have $H \triangleleft H_1$. Finally,

$$|H_1| = |H||H_1/H| = p^i p = p^{i+1}.$$

□

Definition 6.2 (Sylow p-Group) A subgroup P of a group G is said to be a Sylow p-group of G if P is a maximal p-group of G: if $P \subseteq H \subseteq G$ with H being a p-group, then $P = H$.

As a direct consequence of Theorem 6.5, we have

Corollary 6.6 Let G be a group of order $p^n m$ where p is prime, $n \geq 1$, and $\gcd(p, m) = 1$. Let H be a p-subgroup of G. Then

1. H is a Sylow p-group iff $|H| = p^n$
2. Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup
3. If there is only one Sylow p-subgroup, say P, then $P \triangleleft G$

Theorem 6.7 (2nd Sylow Theorem) If H is a p-subgroup of finite group G and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof Let X be the set of all left cosets of P in G and let H act on X by left multiplication. By Lemma 5.7,

$$|X_f| \equiv |X| = [G : P] \pmod{p}.$$

Since $p \not| [G : P]$, we have $|X_f| \neq 0$. Thus, there exists $gP \in X_f$ for some $g \in G$. Then,

$$\begin{aligned} gP \in X_f &\iff hgP = gP \ \forall h \in H \iff g^{-1}hgP = P \ \forall h \in H \\ &\iff gHg^{-1} \subseteq P \iff H \subseteq g^{-1}Pg \end{aligned}$$

If $H$is a Sylow p-subgroup, then $|H| = |P| = |gPg^{-1}|$. So, $H = g^{-1}Pg$. □

Theorem 6.8 (3rd Sylow Theorem) If G is a finite group and p is a prime with $p||G|$, then the number of Sylow p-groups of G divides $|G|$ and is of the form $kp+1$ for some $k \in \mathbb{N} \cup \{0\}$.

Proof By Theorem 6.7, the number of Sylow p-subgroups of G is the number of conjugates of any one of them, say P. This number is $[G : N_G(P)]$ which is a divisor of G. Let X be the set of all Sylow p-subgroups of G and let p act on X by conjugation. Then $q \in X_f$ iff $gQg^{-1} = Q$ for all $g \in P$. The latter condition holds iff $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$. Thus, by Corollary 6.6, they are conjugate in $N_G(Q)$. Since $Q \triangleleft N_G(Q)$, this can only occur if $Q = P$ and $X_f = \{P\}$. By Lemma 5.7,

$$|X| \equiv |X_f| \equiv 1 \pmod{p}$$

thus $|X| = kp + 1$ for some $n \in \mathbb{N} \cup \{0\}$. □

Suppose G is a group with $|G| = p^n m$ where p is prime, $n \geq 0$, and $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups of G. By the 3rd Sylow theorem, we see $n_p | p^n m$ and $n_p \equiv 1 \pmod{p}$. Since $n \not| n_p$, then $n_p | m$.

Example We claim that every group of order 15 is cyclic. To show this, consider group G of order $15 = 3 \times 5$. Let n_p be the number of Sylow p-subgroups of G. By the 3rd Sylow theorem, we have $n_3 | 5$ and $n_3 \equiv 1 \pmod{3}$, so $n_3 = 1$. Similarly, $n_5 | 3$ and $n_5 \equiv 1 \pmod{5}$ so $n_5 = 1$. It follows that there are only one Sylow 3-subgroup and 1 Sylow 5-subgroup, say P_3 and P_5 respectively. So $P_3 \triangleleft G$ and $P_5 \triangleleft G$ by Corollary 6.6. Consider $|P_3 \cap P_5|$ which divides 3 and 5 by Lagrange's Theorem. So $|P_3 \cap P_5| = 1$. Also, $|P_3 P_5| = 15 = |G|$. It follows that

$$G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$

Example We will prove that there are two isomorphism classes of groups of order 21. Let G be a group where $|G| = 21 = 3 \times 7$. Let n_p be the number of Sylow p-groups of G. By the 3rd Sylow Theorem, $n_3 | 7$ and $n_3 \equiv 1 \pmod{7}$. So $n_3 = 1$ or $n_3 = 7$. Also, $n_7 | 3$ and $n_7 \equiv 1 \pmod{3}$ so $n_7 = 1$. It follows that G has a unique Sylow 7-group, say P_7. Note that $P_7 \triangleleft G$ and P_7 is cyclic, say $P_7 = \langle x \rangle$ where $x^7 = 1$. Let H be a Sylow 3-group. Since $|H| = 3$, H is cyclic with $H = \langle y \rangle$ where $y^3 = 1$. Since $P_7 \triangleleft G$, we have $yxy^{-1} = x^i$ for some $0 \leq i \leq 6$. Note that

Week 7.1

$$x = y^3 x y^{-3} = y^2(yxy^{-1})y^{-2} = y^2 x^i y^{-2} = y(yx^i y^{-1})y^{-1} = yx^{i^2} y^{-1} = x^{i^3}.$$

Since $x = x^{i^3}$ and $x^7 = 1$, $i^3 - 1 \equiv 0 \pmod{7}$. Since $0 \leq i \leq 6$, our choices are $i \in \{1, 2, 4\}$. If $i = 1$, then $yxy^{-1} = x$ implies $yx = xy$. So G is abelian and $G \cong \mathbb{Z}_{21}$.

If $i = 2$, then $yxy^{-1} = x^2$, thus

$$G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}.$$

If $i = 4$, then $yxy^{-1} = x^4$. Thus

$$y^2 x y^{-2} = y(yxy^{-1})y^{-1} = yx^4 y^{-1} = x^{16} = x^2$$

Note that y^2 is also a generator of H. Then, by replacing y by y^2, we get back to case 2. It follows that there are 2 isomorphism classes of abelian groups of order 21.

Section 7

Finite Abelian Groups

Subsection 7.1

Primary Decomposition

Given group G and $m \in \mathbb{Z}$, we use the notation

$$G^{(m)} = \{g \in G : g^m = 1\}.$$

Proposition 7.1 Let G be an abelian group. Then $G^{(m)}$ is a subgroup of G.

Proof We have $1 = 1^m \in G^{(m)}$. Also, if $g, h \in G^{(m)}$, since G is abelian, we have

$$(gh)^m = g^m h^m = 1 \text{ and } gh \in G^{(m)}.$$

Finally, if $g \in G^{(m)}$, we have $(g^{-1})^m = g^{-m} = (g^m)^{-1} = 1$, so $g^{-1} \in G^{(m)}$. We are done by the Subgroup Test. □

Proposition 7.2 Let G be a finite abelian group and let $|G| = mk$ where $\gcd(m, k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$
2. $|G^{(m)}| = m$ and $|G^{(k)}| = k$

Proof

1. Since G is abelian, $G^{(m)} \triangleleft G$ and $G^{(k)} \triangleleft G$. Since $\gcd(m, k) = 1$, there exist $x, y \in \mathbb{Z}$ where $mx + ky = 1$. **We will prove a subclaim: $G^{(m)} \cap G^{(k)} = \{1\}$.**

   If $g \in G^{(m)} \cap G^{(k)}$, $g^m = 1 = g^k$. Then

   $$g = g^{mx+ky} = (g^m)^x (G^k)^y = 1^x 1^y = 1.$$

   We will prove another subclaim: $G = G^{(m)} G^{(k)}$.

   If $g \in G$, then $1 = g^{mk} = (g^k)^m = (g^m)^k$. It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Then

   $$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}.$$

   Combining the two subclaims, by Theorem 3.13 we have

   $$G \cong G^{(m)} \times G^{(k)}.$$

2. Write $|G^{(m)}| = m'$ and $|G^{(k)}| = k'$. By (1), $mk = |G| = m'k'$.

   Claim: $\gcd(m, k') = 1$.

   Suppose $\gcd(m, k') \neq 1$. So there exists a prime p where $p|m$ and $p|k'$. By Cauchy's Theorem, there exists $g \in G^{(k)}$ where $o(g) = p$. Since $p|m$, we have $g^m = (g^p)^{m/p} = 1$ so $g \in G^{(m)}$. But we proved that $g \in G^{(k)} \cap G^{(m)} = \{1\}$, but $o(g) = p$: contradiction.

Now that we have shown $\gcd(m, k') = 1$, since $m|m'k'$, we have $m|m'$ and similarly we can show $k|k'$. So $m = m'$ and $k = k'$.

□

As a direct consequence of Proposition 3.2, Week 7.2

Theorem 7.3 (Primary Decomposition) Let G be a finite abelian group where

$$|G| = p_1^{n_1}...p_k^{n_k}$$

such that $p_1, ..., p_k$ are distinct primes and $n_1, ..., n_k \in \mathbb{N}$. Then, we have

1. $G \cong G^{(p_1^{n_1})} \times ... \times G^{(p_k^{n_k})}$
2. $|G^{(p_i^{n_i})}| = p_i^{n_i}$ for each $i = 1, ..., k$

Example Let $G = \mathbb{Z}_{13}^*$. We know $|G| = 12 = 2^3 3$. As an exercise, we can show

$$G^{(4)} = \{1, 5, 8, 12\} \text{ and } G^{(3)} = \{1, 3, 9\}.$$

Then, by Theorem 7.3, we have $\mathbb{Z}_{13}^* = \{1, 5, 8, 12\} \times \{1, 3, 9\}$.

Subsection 7.2

Structure Theorem of Finite Abelian Groups

By Theorem 7.3, to understand finite abelian groups, it sufficies to consider finite abelian groups of prime power order. We recall that if $|G| = p$, then $G \cong \mathbb{Z}_p$. Also, if $|G| = p^2$, then either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proposition 7.4 If G is a finite abelian p-group that contains only 1 subgroup of order p, then G is cyclic.

Proof Let $y \in G$ be of maximal order (so $o(y) \geq o(x)$ for any $x \in G$). Our claim is that $G = \langle y \rangle$.

For the sake of contradiction, assume $G \neq \langle y \rangle$. Then $G/\langle y \rangle$ is a non-trivial p-group which contains an element z of order p by Cauchy's Theorem. In particular, $z \neq 1$. Consider the coset map $\pi : G \to G/\langle y \rangle$ and let $x \in G$ such that $\pi(x) = z$. Since $\pi(x^p) = \pi(x)^p = z^p = 1$, we see that $x^p \in \langle y \rangle$. This implies that $x^p = y^m$ for some $m \in \mathbb{Z}$. We now have two cases:

1. If $p \not| m$, since $o(y) = p^r$ for some $r \in \mathbb{N}$, by Proposition 2.8 $o(y^m) = o(y) = p^r$. Since y is of maximal order,

   $$o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$$

   which is a contradiction.

2. If $p|m$, $m = pk$ for some $k \in \mathbb{Z}$. Thus, we have $x^p = y^m = y^{pk}$. Since G is abelian, $(xy^{-k})^p = 1$. Thus, xy^{-k} belongs to the one and only subgroup of order p, say H. On the other hand, cyclic group $\langle y \rangle$ contains a subgroup of order p which must be the one and only H. Thus, $xy^{-k} \in \langle y \rangle$ which implies $x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$, a contradiction.

Since both cases led to contradiction, $G = \langle y \rangle$ and so is cyclic. □

Proposition 7.5 Let $G \neq \{1\}$ be a finite p-group. Let C be a cyclic subgroup of maximum order. Then G contains a subgroup B such that $G = CB$ and $C \cap B = \{1\}$. Thus, by Theorem 3.13, $G \cong C \times B$.

Proof We use a proof by induction. If $|G| = p$, we take $C = G$ and $B = \{1\}$, and the result follows. Suppose the result holds for all abelian groups of order p^{n-1} where $n \in \mathbb{N}$ and $n \geq 2$. Consider $|G| = p^n$. There are two cases:

1. If $G = C$, then take $B = \{1\}$. The result follows.
2. If $G \neq C$, then G is not cyclic. By Proposition 7.4, at least 2 subgroups exist of order p. Since C is cyclic, by Theorem 2.12, it contains exactly one subgroup of order p. Thus there exists a subgroup D of G with $|D| = p$ and $D \not\subseteq C$. Since $|D| = p$ and $D \not\subseteq C$, we have $C \cap D = \{1\}$. Consider the coset map $\pi : G \to G/D$. If we consider $\pi|_C$ (the restriction of π on C), then

$$\ker \pi|_C = C \cap D = \{1\}$$

and so by the 1st isomorphism theorem, $\pi(C) \cong C$. Let y be a generator of C where $C = \langle y \rangle$. Since $\pi(C) \cong C$, then $\pi(C) = \langle \pi(y) \rangle$. By the assumption on C, $\pi(C)$ is a cyclic group of G/D of max order. Since $|G/D| = p^{n-1}$, by the inductive hypothesis, G/D has subgroup E where $\pi(C)E = G/D$ and $\pi(C) \cap E = \{1\}$. Let $B = \pi^{-1}(E)$ where $\pi(B) = E$.

Claim 1: $G = CB$

Note that since E is a subgroup containing $\{1\}$, $\pi^{-1}(\{1\}) = D \subseteq B$. If $x \in G$, since $\pi(C)\pi(B) = \pi(C)E = G/D$, there exists $u \in C$ and $v \in B$ such that $\pi(x) = \pi(u)\pi(v)$. Since $\pi(xu^{-1}v^{-1}) = 1$, then $xu^{-1}v^{-1} \in D \subseteq B$. Since $v \in B$, $xu^{-1} \in B$. Since G is abelian, $x = uxu^{-1} \in CB$.

Claim 2: $C \cap B = \{1\}$.

Let $x \in C \cap B$. Then $\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}$.

By Claim 1 and 2, the result follows.

□

Theorem 7.6 Let $G \neq \{1\}$ be a finite p-group. Then G is isomorphic to a direct product of cyclic groups.

Proof By Proposition 7.5, there exist cyclic group C_1 and subgroup B_1 of G such that $G \cong C_1 \times B_1$. Since $|B_1||G|$ by Lagrange's Theorem, B_1 is also a p-group. If $B_1 \neq \{1\}$, then by Proposition 7.5 once again, there exist cyclic group C_2 and subgroup B_2 such that $B_1 \cong C_2 \times B_2$. Continuing this a finite number of times k gets cyclic groups $C_1, ..., C_k$ til $B_k = \{1\}$. Then

$$G \cong C_1 \times ... \times C_k.$$

□

Remark: one can show that the decomposition of finite abelian p-groups into direct products of cyclic groups is unique up to their order. Moreover, one can show (exercise)

that if G is a finite abelian p-group and

$$G \cong C_1 \times ... \times C_k \cong D_1 \times ... \times D_\ell$$

are two decompositions of G as products of cyclic groups C_i and D_j of order p^{n_i} and p^{m_j} respectively, then $k = \ell$ and after a suitable rearrangement,

$$n_1 = m_1, ..., n_k = m_k.$$

No lecture (Test 1). Week 7.3

Theorem 7.7 (Structure Theorem of Finite Abelian Groups) If G is a finite abelian group, then Week 8.1

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times ... \times \mathbb{Z}_{p_k^{n_k}}$$

where

$$\mathbb{Z}_{p_i^{n_i}} = (\mathbb{Z}_{p_i^{n_i}}, +) \cong C_{p_i^{n_i}}$$

are cyclic groups of order $p_i^{n_i}$ for $1 \leq i \leq k$.

Note that the p_i's are not necessarily distinct. The numbers $p_i^{n_i}$ are uniquely determined up to their order. Note that if p_1, p_2 are distinct powers,

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}},$$

hence we have

Theorem 7.8 (Invariant Factor Decomposition of Finite Abelian Groups) Let G be a finite abelian group, then

$$G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$$

where $n_i \in \mathbb{N}$ for $1 \leq i \leq r$, $n_i > 1$, and

$$n_1 | n_2 | ... | n_r.$$

Example Consider all abelian groups of order $48 = 2^4 3$. By Theorem 7.3, we have $G \cong H \times \mathbb{Z}_3$ where H is an abelian group of order 2^4. The options for H are

$$\mathbb{Z}_{2^4}, \mathbb{Z}_{2^3} \times \mathbb{Z}_2, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}, \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Thus, we have

$$\begin{aligned}
G &\cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48} \\
G &\cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24} \\
G &\cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_{12} \\
G &\cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12} \\
G &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6
\end{aligned}$$

by combining highest powers.

Section 8

Rings

Subsection 8.1

Rings

Definition 8.1 (Ring) A set R is a (unitary) ring if it has 2 operations, addition $+$ and multiplication $*$ such that $(R, +)$ is an abelian group and $(R, *)$ satisfies closure, associativity, and identity properties of a group in addition to a distribution law. More precisely, if R is a ring, $\forall a, b, c \in R$:

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. There exists $0 \in R$ such that $a + 0 = a = 0 + a$ (the zero of R)
5. There exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$ (inverse of a)
6. $ab := a * b \in R$
7. $a(bc) = (ab)c$
8. There exists $a \in R$ such that $a1 = a = 1a$ (the unity of R)
9. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ (distributive law)

Week 8.2

The ring R is said to be a commutative ring if it also satisfies $ab = ba$ for all $a, b \in R$.

Example | $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings with the zero being 0, and the unity being 1.

Example | For $n \in \mathbb{N}$ where $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with the zero being $[0]$ and the unity being $[1]$.

Example | For $n \in \mathbb{N}$ with $n \geq 2$, the set $M_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication. The zero is the 0 matrix and the unity is the identity matrix.

Warning: since $(R, *)$ is not a group, there is no left or right cancellation. For example, in $\mathbb{Z}$, $0 * x = 0 = 0 * y$ does not imply $x = y$.

Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N}$ and $a \in \mathbb{R}$, we write

$$\begin{aligned} na &= a + ... + a && n \text{ times addition} \\ a^n &= a * a * ... * a && n \text{ times multiplication} \end{aligned}$$

We recall that for a group G and $g \in G$, $g^0 = 1$, $g^1 = g$, and $(g^{-1})^{-1} = g$. Thus, for addition, $0a = 0$, $1 * a = a$, and $-(-a) = a$ where $a \in R$. Also, for $n \in \mathbb{N}$, we say

$$(-n)a = (-a) + ... + (-a).$$

We also define $a^0 = 1$. If the multiplicative inverse of a exists (note that it does not necessarily exist), we write a^{-1} where $a^{-1}a = 1 = aa^{-1}$. We also use the notion

$a^{-n} = (a^{-1})^n$. Also, by Proposition 1.2, for $n, m \in \mathbb{Z}$, we have $(na) + (ma) = (n+m)a$, $n(ma) = (nm)a$, and $n(a+b) = na + nb$. One can prove

Proposition 8.1 Let R be a ring and $r, s \in R$.

1. If 0 is the zero of R, $0r = 0 = r0$
2. $(-r)s = r(-s) = -(rs)$
3. $(-r)(-s) = rs$
4. For all $m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$

Definition 8.2 (Trivial Ring) A trivial ring is a ring of only 1 element. In this case, we have $1 = 0$.

Remark: if R is a ring where $R \neq \{0\}$, since $r = r * 1$ for all $r \in R$, we have $1 \neq 0$ (otherwise $r = r1 = r0 = 0$ by Proposition 8.1).

Example Let $R_1, ..., R_n$ be rings. We define the componentwise operations on the product $R_1 \times ... \times R_n$ as follows:

$$(r_1, ..., r_n) + (s_1, ..., s_n) = (r_1 + s_1, ..., r_n + s_n)$$
$$(r_1, ..., r_n) * (s_1, ..., s_n) = (r_1 s_1, ..., r_n s_n)$$

One can check that $R_1 \times ... \times R_n$ is a ring, with the zero being $(0_{R_1}, ..., 0_{R_n})$ and the unity being $(1_{R_1}, ..., 1_{R_n})$. The set $R_1 \times ... \times R_n$ is called the direct product of $R_1, ..., R_n$.

Definition 8.3 (Characteristic) If R is a ring, we define the characteristic of R, denoted $\text{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$:

$$\text{ch}(R) = \begin{cases} n & o(1_R) = n \in \mathbb{N} \\ 0 & o(1_r) = \infty \end{cases}$$

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean $kr = 0$ for all $r \in R$. By Proposition 8.1, we have

$$kr = k(1_R r) = (k1_R)r$$

so $kR = 0$ iff $k1_R = 0$. By Proposition 2.6 and 2.7,

Proposition 8.2 Let R be a ring and $k \in \mathbb{Z}$.

1. If $\text{ch}(R) = n \in \mathbb{N}$, then $kR = 0$ iff $n|k$
2. If $\text{ch}(R) = 0$, then $kR = 0$ iff $k = 0$

Example Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0. For $n \in \mathbb{N}$, where $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic n.

Subsection 8.2
Subrings

Definition 8.4 (Subring) A subset S of a ring R is a subring if S is a ring itself with $1_S = 1_R$, along with the same $+$ and $*$.

Week 8.3

Note that properties 2, 3, 7, and 9 of rings are automatically satisfied. Thus, to show S is a subring, it suffices to show:

Definition 8.5 (Subring Test) A subset S of a ring R is a subring if

1. $1_R \in S$
2. If $s, t \in S$, then $s - t \in S$ and $st \in S$

Note that if (2) holds, then $0 = s - s \in S$ and $-t = 0 - t \in S$.

Example We have a chain of commutative rings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Example If R is a ring, the center $Z(R)$ of R is defined

$$Z(R) = \{z \in R : zr = rz \ \forall r \in R\}.$$

Note that $1_R \in Z(R)$. Also, if $s, t \in Z(R)$, for all $r \in R$ we have

$$(st)r = s(tr) = s(rt) = (rs)t = r(st)$$

and

$$(s - t)r = sr - tr = rs - rt = r(s - t)$$

so by the Subring Test, $Z(R)$ is a subring of R.

Example Let

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}.$$

Then one can show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, called the ring of Gaussian integers.

Subsection 8.3
Ideals

Let R be a ring, and let A be an additive subgroup of R. Since $(R, +)$ is abelian, $A \triangleleft R$. Thus, we have the additive quotient group

$$R/A = \{r + A : r \in R\} \text{ where } r + A = \{r + a : a \in A\}.$$

Using the known properties about cosets and quotient groups, we have

Proposition 8.3 Let R be a ring and let A be an additive subgroup of R. For $r, s \in R$,

1. $r + A = s + A$ iff $(r - s) \in A$
2. $(r + A) + (s + A) = (r + s) + A$
3. $0 + A = A$ (0 is the additive identity of R/A)
4. $-(r + A) = (-r) + A$ ($(-r) + A$ is the additive inverse of $r + A$)
5. $k(r + A) = kr + A$ for all $k \in \mathbb{Z}$

Since R is a ring, it is natural to ask if we can make R/A to be a ring. A natural way to define multiplication in R/A is

$$(r + A)(s + A) = rs + A$$

for all $r, s \in A$. Note that we could have $r + A = r_1 + A$ and $s_1 + A = s + A$ where $r \neq r_1$ and $s \neq s_1$ are elements of R. Thus, in order to make this multiplication make sense, a necessary condition is that

$$r + A = r_1 + A \text{ and } s + A = s_1 + A \Longrightarrow rs + A = r_1 s_1 + A.$$

If this holds, we say that the multiplication is well defined.

Proposition 8.4 Let A be an additive subgroup of ring R. For $a \in A$, define $Ra = \{ra : r \in R\}$ and $aR = \{ar : r \in R\}$. The following are equivalent:

1. $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$
2. For $r, s \in R$, $(r + A)(s + A) = rs + A$ is well defined in R/A.

PROOF (1) $\Longrightarrow$ (2). Let $r + A = r_1 + A$ and $s + A = s_1 + A$ for some $r \neq r_1$ and $s \neq s_1$ in A. We want to show that $rs + A = r_1 s_1 + A$. Since $(r - r_1) \in A$ and $(s - s_1) \in A$,

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \\ &\subseteq A \end{aligned}$$

By Proposition 8.3 (1), we have $rs + A = r_1 s_1 + A$.

(2) $\Longrightarrow$ (1). Let $r \in R$ and $a \in A$. By Proposition 8.2 (1),

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = 0 + A = A.$$

Thus, $ra \in A$ so $Ra \subseteq A$. Similarly, we can show $aR \subseteq A$. □

Definition 8.6 (Ideal) An additive subgroup A of ring R is an ideal of R if $Ra \subseteq A$ (left ideal) and $aR \subseteq A$ (right ideal) for all $a \in A$. Thus, a subset A of R is an ideal if $0 \in A$ and for $a, b \in A$ and $r \in R$, we have $a - b \in A$ and $ra, ar \in A$.

Example If R is a ring, then $\{0\}$ and R are ideals of R.

Example Let R be a commutative ring an $a_1, ..., a_n \in R$, then consider the set I generated by $a_1, ..., a_n$:

$$I = \langle a_1, ..., a_n \rangle = \{r_1 a_1 + ... + r_n a_n : r_i \in R\}.$$

One can show that I is an ideal.

Proposition 8.5 Let A be an ideal of ring R. If $1_R \in A$, then $A = R$. Week 9.1

PROOF For every $r \in R$, since A is an ideal and $1_R \in A$, we have $r = r1_R \in A$. It follows that $R \subseteq A \subseteq R$ so $A = R$. □

Remark: By Proposition 8.5, we see that ideals are not necessarily a ring since it misses the unity 1_R.

Proposition 8.6 Let A be an ideal of ring R. Then the additive quotient group R/A is a ring with the multiplication

$$(r + A)(s + A) = rs + A,$$

and the unity of R/A is $(1 + A)$.

Definition 8.7 (Quotient Ring) Let A be an ideal of ring R. The ring R/A is called the quotient ring of R by A.

Definition 8.8 (Principal Ideal) Let R be a commutative ring and A be an ideal of R. If $A = aR = Ra$ for some $a \in A$, we say A is a principal ideal generated by a and denote it by $A = \langle a \rangle$.

Example If $n \in \mathbb{Z}$, then $\langle n \rangle = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proposition 8.7 All ideals of $\mathbb{Z}$ are of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$. If $\langle n \rangle \neq \{0\}$ and $n \in \mathbb{N}$, then the generator is uniquely determined.

PROOF Let A be an ideal of $\mathbb{Z}$. If $A = \{0\}$, then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ where $|a|$ is minimal. Clearly, we have $\langle a \rangle \subseteq A$. For the other inclusion, let $b \in A$. By the division algorithm, write $b = qa + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$. If r is non-zero, since A is an ideal and $a, b \in A$, we have

$$r = b - qa \in A$$

with $|r| < |a|$. This is a contradiction, so $r = 0$ and $b = qa$ and $b \in \langle a \rangle$. It follows that $A = \langle a \rangle$. □

SUBSECTION 8.4

Isomorphism Theorems

Definition 8.9 (Ring Homomorphism) Let R and S be rings. A mapping $\theta : R \to S$ is a ring homomorphism if for all $a, b \in R$,

1. $\theta(a + b) = \theta(a) + \theta(b)$
2. $\theta(ab) = \theta(a)\theta(b)$
3. $\theta(1_R) = 1_S$

Remark: Condition (2) does not imply (3) since $\theta(1_R) \in S$ does not necessarily have a multiplicative inverse. So, although by (2), we have $\theta(1_R) = \theta(1_R)\theta(1_R)$, this does not imply $\theta(1_R) = 1_S$.

Example The mapping $k \mapsto [k]$ from $\mathbb{Z}$ to $\mathbb{Z}_n$ is an onto ring homomorphism.

Example If R_1 and R_2 are rings, the projection $\pi_1 : R_1 \times R_2 \to R_1$ defined $\pi_1(r_1, r_2) = r_1$ is an onto ring homomorphism. Similarly, $\pi_2 : R_1 \times R_2 \to R_2$ defined $\pi_2(r_1, r_2) = r_2$ is also an onto ring homomorphism.

Proposition 8.8 Let $\theta : R \to S$ be a ring homomorphism, and $r \in R$:

1. $\theta(0_R) = 0_S$
2. $\theta(-r) = -\theta(r)$
3. $\theta(kr) = k\theta(r)$ for $k \in \mathbb{Z}$
4. $\theta(r^n) = \theta(r)^n$ for $n \in \mathbb{N} \cup \{0\}$
5. If $u \in R^*$ (the set of elements of R with multiplicative inverses), where u is called a unit of R, then $\theta(u^k) = \theta(u)^k$ for $k \in \mathbb{Z}$

Definition 8.10 (Ring Isomorphism) A mapping of rings $\theta : R \to S$ is a ring isomorphism if θ is a homomorphism and a bijection. In this case, we say R and S are isomorphic and denoted as $R \cong S$.

Definition 8.11 (Kernel and Image) Let $\theta : R \to S$ be a ring homomorphism. The kernel of θ is defined

$$\ker\theta = \{r \in R : \theta(r) = 0\} \subseteq R$$

and the image of θ is

$$\operatorname{im}\theta = \theta(R) = \{\theta(r) : r \in R\} \subseteq S.$$

Week 9.2

We learned from group theory that $\ker\theta$ and $\operatorname{im}\theta$ are additive subgroups of R and S respectively.

Proposition 8.9 Let $\theta : R \to S$ be a ring homomorphism.

1. $\operatorname{im}\theta$ is a subring of S
2. $\ker\theta$ is an ideal of R

PROOF

1. Since $\operatorname{im}\theta = \theta(R)$ is an addditive subgroup of S, it suffices to show that $\theta(R)$ is closed under multiplication and $1_S \in \theta(R)$ by the Subring Test. Note that $1_S = \theta(1_R) \in \theta(R)$. Also, if $s_1 = \theta(r_1)$ and $s_2 = \theta(r_2)$, we have $s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R)$.
2. Since $\ker\theta$ is an additive subgroup of R, it suffices to show that $ra, ar \in \ker\theta$ for all $r \in R$ and $a \in \ker\theta$. Let $r \in R$ and $a \in \ker\theta$, then $\theta(ra) = \theta(r)\theta(a) = \theta(r) \times 0 = 0$ so $ra \in \ker\theta$. Similarly, we can show $ar \in \ker\theta$.

□

Theorem 8.10 (1st Isomorphism Theorem) Let $\theta : R \to S$ be a ring homomorphism. We have

$$R/\ker\theta \cong \operatorname{im}\theta.$$

PROOF Let $A = \ker\theta$. Since A is an ideal of R, R/A is a ring. Define the ring map $\bar{\theta} : R/A \to \operatorname{im}\theta$ by $\bar{\theta}(r + A) = \theta(r)$ for all $r + A \in R/A$. Note that

$$r + A = s + A \iff r - s \in A \iff \theta(r - s) = 0 \iff \theta(r) = \theta(s)$$

so $\bar{\theta}$ is well defined as one-to-one. Also, $\bar{\theta}$ is clearly onto. One can show that $\bar{\theta}$ is a

ring homomorphism (exercise). It follows that $\bar{\theta}$ is a ring isomorphism and so

$$R/\ker\theta \cong \operatorname{im}\theta.$$

□

Let A and B be subsets of a ring R. If both A and B are subrings, then $A \cap B$ is the "largest" subring of R contained in both A and B. To consider the "smallest" subring of R containing both A and B where A and B are not necessarily subrings, define the sum

$$A + B = \{a + b : a \in A, b \in B\}.$$

Then, one can show

Proposition 8.11 If R is a ring and A and B are subsets of R,

1. If A and B are two subrings of R, $A \cap B$ is a subring of R
2. If A is a subring and B is an ideal of R, then $A + B$ is a subring of R
3. If A and B are ideals of R, $A + B$ is an ideal of R

Theorem 8.12 (2nd Isomorphism Theorem) Let A be a subring and B be an ideal of R. Then $A+B$ is a subring of R, B is an ideal of $A + B$, $A \cap B$ is an ideal of A, and

$$(A + B)/B \cong A/(A \cap B).$$

Theorem 8.13 (3rd Isomorphism Theorem) Let A and B be ideals of ring R and $A \subseteq B$. Then B/A is an ideal in R/A and

$$(R/A)/(B/A) \cong R/B.$$

Theorem 8.14 (Chinese Remainder Theorem) Let A and B be ideals of R.

1. If $A + B = R$, then
$$R/(A \cap B) \cong R/A \times R/B$$
2. If $A + B = R$ and $A \cap B = \{0\}$, then
$$R \cong R/A \times R/B$$

PROOF Note that (2) is a direct consequence of (1), so it suffices to prove (1). Define $\theta : R \to R/A \times R/B$ by $\theta(r) = (r + A, r + B)$ for all $r \in R$. As an exercise, we can show that θ is a ring homomorphism. Also, $\ker\theta = A \cap B$. To show that θ is onto, let $(s + A, t + B) \in R/A \times R/B$ where $s, t \in R$. Since $A + B = R$, there exists $a \in A$ and $b \in B$ where $a + b = 1$. Let $r = sb + ta$, then

$$s - r = s - sb - ta = s(1 - b) - ta = sa - ta = (s - t)a \in A.$$

Thus, $s + A = r + A$. Similarly, $t + B = r + B$. Thus,

$$\theta(r) = (r + A, r + B) = (s + A, t + B).$$

By the 1st Isomorphism Theorem,

$$R/(A \cap B) \cong R/A \times R/B.$$

□

Let $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. By Euclid's Lemma, $1 = mr + ns$ for some $r, s \in \mathbb{Z}$. Then $1 \in m\mathbb{Z} + n\mathbb{Z}$ and hence $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Also, since $\gcd(m, n) = 1$, $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. By Chinese Remainder Theorem,

Corollary 8.15

1. If $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$
2. If $m, n \in \mathbb{N}$ where $m, n \geq 2$ and $\gcd(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n)$$

where $\phi(m) = |\mathbb{Z}_m^*|$ is the Euler ϕ-function.

Remark: By Corollary 8.15, for $[a] \in \mathbb{Z}_m$ and $[n] \in \mathbb{Z}_n$, there exists a unique $[c] \in \mathbb{Z}_{mn}$ such that $[c] = [a]$ in $\mathbb{Z}_m$ and $[c] = [b]$ in $\mathbb{Z}_n$. This is equivalent to saying that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution $x \equiv c \pmod{mn}$.

Example Combining the 3rd Isomorphism Theorem and the fact that all ideals of $\mathbb{Z}$ are principal, we can say all ideals of $\mathbb{Z}_n$ are principal. Week 9.3

Let p be a prime. Recall that one consequence of Lagrange's Theorem is that every group G of order p is cyclic: $G \cong C_p \cong \mathbb{Z}_p$. We have an analogous result for rings:

Proposition 8.16 If R is a ring with $|R| = p$ where p is prime, then $R \cong \mathbb{Z}_p$.

PROOF Define $\theta : \mathbb{Z}_p \to R$ as $\theta([k]) = k1_R$. Note that since R is an additive group and $|R| = p$, we have $o(1_R) = 1$ or $o(1_R) = p$ by Lagrange's Theorem. Since $1_R \neq 0$, we have $o(1_R) = p$. Thus,

$$[k] = [m] \iff p|(k - m) \iff (k - m)1_R = 0 \iff k1_R = m1_R$$

so θ is well-defined and one-to-one. Also, θ is a ring homomorphism (exercise). Since $|\mathbb{Z}_p| = p = |R|$, then θ is onto, so it follows that θ is a ring isomorphism and $R \cong \mathbb{Z}_p$. □

Section 9

Commutative Rings

Subsection 9.1

Integral Domains and Fields

Definition 9.1 (Unit) Let R be a ring. We say $u \in R$ is a unit if u has a multiplicative inverse in R, denoted u^{-1}. We have $uu^{-1} = 1 = u^{-1}u$.

Note that if u is a unit in R, and $r, s \in R$, we have $ur = us \implies r = s$ and $ru = su \implies r = s$. Let R^* denote the set of all units in R. One can show that $(R^*, *)$ is a group called the group of units of R.

Example | Note that 2 is a unit in $\mathbb{Q}$ but not a unit in $\mathbb{Z}$. We have $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ and $\mathbb{Z}^* = \{\pm 1\}$.

Example | Consider the ring of Gaussian integers $\mathbb{Z}[i]$. One can show that $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Definition 9.2 (Division Ring) A ring $R \neq \{0\}$ is a division ring if $R^* = R\backslash\{0\}$.

Definition 9.3 (Field) A field is a commutative division ring.

Example | $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields but not $\mathbb{Z}$.

Example | We recall that the equation $[a][x] = [1]$ in $\mathbb{Z}_n$ has a solution iff $\gcd(a, n) = 1$. Thus, if $n = p$ is a prime, $\gcd(a, p) = 1$ for all $a \in \{1, ..., p-1\}$. Thus, $\mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$ and $\mathbb{Z}_p$ is a field. However, if n is not prime, then we can write $n = ab$ where $1 < a, b < n$. Then the non-zero congruence classes $[a]$ and $[b]$ are not units in $\mathbb{Z}_n$ as there is no solution $[a][x] = [1]$ or $[b][x] = [1]$ and hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n\backslash\{0\}$. Thus, $\mathbb{Z}_n$ is a field iff n is prime.

Remark: If R is a field, its only ideals are $\{0\}$ and R since if $A \neq \{0\}$ is an ideal of R, then $0 \neq a \in A$ implies $aa^{-1} = 1 \in A$. By Proposition 8.5, we have $A = R$. As a consequence, if we have a ring homomorphism θ from a field F to a ring S, since $\ker\theta$ is an ideal, $\ker\theta$ is either 0 or F. Hence, θ is either injective of a zero map.

Example | One can prove Wedderburn's Little Theorem, which states that every finite division ring is a field.

Note that to solve the equation $x^2 - x - 6 = 0$ in $\mathbb{Z}$, we factor $(x-3)(x+2) = 0$ which gives $x = 3$ or $x = -2$. However, the same does not hold in general: take $\mathbb{Z}_6$ for example. We see that $[2][3] = 0$ hence if we have $[x-3][x+2] = 0$, it does not necessarily mean $[x] = [3]$ or $[x] = [-2]$. This example motivates the following definition: Week 10.1

Definition 9.4 (Zero Divisor) Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$, we say a is a zero divisor if there exists $0 \neq b \in R$ such that $ab = 0$.

Example | In $\mathbb{Z}_6$, $[2], [3], [4]$ are zero divisors since $[2][3] = [0] = [4][3]$.

Example | The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{R})$ since

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

Proposition 9.1 Given a ring R with $a, b, c \in R$, the following are equivalent:

1. If $ab = 0$ in R, then $a = 0$ or $b = 0$
2. If $ab = ac$ in R and $a \neq 0$, then $b = c$
3. If $ba = ca$ in R and $a \neq 0$, then $b = c$

Proof We will prove (1) $\iff$ (2). The proof for (1) $\iff$ (3) is similar.

(1) $\implies$ (2). Let $ab = ac$ where $a \neq 0$. Then $a(b - c) = 0$. By 1, since $a \neq 0$, then $b - c = 0$.

(2) $\implies$ (1). Let $ab = 0$. If $a = 0$, we are done. Suppose $a \neq 0$, then $ab = 0 = a0$. By (2), $b = 0$. □

Definition 9.5 (Integral Domain) A commutative ring $R \neq \{0\}$ is an integral domain if it has no zero divisors; i.e. if $ab = 0$ in R, then $a = 0$ or $b = 0$.

Example $\mathbb{Z}$ is an integral domain.

Example If p is prime, then $p|ab$ implies $p|a$ or $p|b$ from a result in MATH 135/145. This means $[a][b] = [0]$ in $\mathbb{Z}_p$ implies $[a] = [0]$ or $[b] = [0]$. However, if $n = ab$ with $1 < a, b < n$, then $[a][b] = [0]$ with $[a] \neq [0]$ and $[b] \neq [0]$. Thus, $\mathbb{Z}_n$ is an integral domain iff n is prime.

Proposition 9.2 Every field is an integral domain.

Proof Let $ab = 0$ in a field R. Suppose $a \neq 0$. Since R is a field, $a \in R^*$ and $a^{-1} \in R$ exists. Then

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

□

Remark: Using the same proof, we can show that every subring of a field is an integral domain.

Example The Gaussian ring $\mathbb{Z}[i]$ is an integral domain. Since $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$, then $\mathbb{Z}[i]$ is not a field.

Proposition 9.3 Every finite integral domain is a field.

Proof Let R be a finite integral domain and $0 \neq a \in \mathbb{R}$. Consider the map $\theta : R \to R$ given by $\theta(r) = ar$. Since R is an integral domain, $ar = as$ and $a \neq 0$ implies $r = s$. Hence, θ is injective. In particular, there exists $b \in R$ such that $ab = 1$. Since R is commutative, $ab = 1 = ba$ so a is a unit. Thus $R^* = R\backslash\{0\}$ and so R is a field. □

Proposition 9.4 The characteristic of any integral domain is either 0 or a prime p.

Proof Let R be an integral domain. There are two cases: if $\text{ch}(R) = 0$, we are done. So suppose $\text{ch}(R) = n \in \mathbb{N}$. Since $R \neq \{0\}$, we have $n \neq 1$. Suppose n is not prime, so we can write $n = ab$ where $1 < a, b < n$. If 1 is the unity of R, then by Proposition 8.1, we have

$$(a \cdot 1)(b \cdot 1) = ab(1 \cdot 1) = n \cdot 1 = 0.$$

Since R is an integral domain, this means either $a \cdot 1 = 0$ or $b \cdot 1 = 0$. This is a contradiction since $o(1_R) = n$ and $a, b < n$. Thus n is a prime. □

Remark: Let R be an integral domain where $\text{ch}(R) = p$, a prime. For $a, b \in R$, we have Week 10.2

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + ... + \binom{p}{p}b^p$$

by the binomial theorem, and since p is a prime, we have $p|\binom{p}{i}$ for each $1 \leq i \leq p-1$. Since $\text{ch}(R) = p$, we must have

$$(a+b)^p = a^p + b^p.$$

Subsection 9.2

Prime Ideals and Maximal Ideals

Let p be a prime and $a, b \in \mathbb{Z}$. Recall that $p|ab$ implies that $p|a$ or $p|b$. In other words, if $ab \in p\mathbb{Z}$, then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Definition 9.6 (Prime Ideal) Let R be a commutative ring. An ideal $P \neq R$ of R is a prime ideal if whenever $r, s \in R$ satisfies $rs \in P$, then $r \in P$ or $s \in P$.

Example $\{0\}$ is a prime ideal of $\mathbb{Z}$.

Example For $n \in \mathbb{N}$ where $n \geq 2$, $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ iff n is prime.

Proposition 9.5 If R is a commutative ring, then an ideal P of R is a prime ideal iff R/P is an integral domain.

Proof Since R is a commutative ring, so is R/P. Note that

$$R/P \neq \{0\} \iff 0+P \neq 1+P \iff 1 \notin P \iff P \neq R.$$

Also, for $r, s \in R$, we have that P is a prime ideal $\iff rs \in P$ implies $r \in P$ or $s \in P \iff (r+P)(s+P) = 0+P$ implies $r+P = 0+P$ or $s+P = 0+P \iff R/P$ is an integral domain. □

Definition 9.7 (Maximal Ideal) Let R be a commutative ring. An ideal $M \neq R$ of R is a maximal ideal if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Remark: Let M be a maximal ideal of R and let $r \notin M$. Then the ideal $\langle r \rangle + M$ is equal to R since $M \subseteq \langle r \rangle + M \subseteq R$ and $M \neq \langle r \rangle + M$.

Proposition 9.6 If R is a commutative ring, then an ideal M of R is a maximal ideal iff R/M is a field.

Proof Since R is a commutative ring, so is R/M. Note that

$$R/M \neq \{0\} \iff 0+M \neq 1+M \iff 1 \notin M \iff M \neq R.$$

Also, for $r \in R$, note that $r \notin M$ iff $r + M \neq 0 + M$. So,

$$\begin{aligned} M \text{ is a maximal ideal} &\iff \langle r \rangle + M = R \text{ for any } r \notin M \\ &\iff 1 \in \langle r \rangle + M \text{ for all } r \notin M \\ &\iff \forall r \notin M, \text{ exists } s \in R \text{ such that } 1 + M = rs + M \\ &\iff \forall r + m \neq 0 + M, \exists s + M \in R/M \text{ s.t. } (r + M)(s + M) = 1 + M \\ &\iff R/M \text{ is a field} \end{aligned}$$

□

Combining Proposition 9.2, 9.5, and 9.6, we have

Corollary 9.7 Every maximal ideal of a commutative ring is a prime ideal.

Remark: The converse of Corollary 9.7 is not true. For example, in $\mathbb{Z}$, $\{0\}$ is a prime ideal, but not a maximal ideal.

Example Consider the ideal $\langle x^2 + 1 \rangle$ in the ring $\mathbb{Z}[x]$. The map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined $\theta(f(x)) = f(i)$ is surjective since $\theta(a + bx) = a + bi$ for any $a, b \in \mathbb{Z}$. Also, one can check that the kernel of the map is $\langle x^2 + 1 \rangle$. By the 1st Isomorphism Theorem,

$$\mathbb{Z}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Z}[i].$$

Since $\mathbb{Z}[i]$ is an integral domain but not a field, we conclude that $\langle x^2 + 1 \rangle$ is a prime ideal but not maximal.

SUBSECTION 9.3

Fields of Fractions

We have seen that every subring of a field is an integral domain. The converse also holds: every integral domain is isomorphic to a subring of a field.

Our goal: given an integral domain R, we want to construct a field F of all the fractions $\frac{r}{s}$ from R. Week 10.3

Let R be an integral domain and let $D = R \backslash \{0\}$. Consider the set

$$X = R \times D = \{(r, s) : r \in R, s \in D\}.$$

We say that $(r, s) \equiv (r_1, s_1)$ iff $rs_1 = r_1 s$. One can show that $\equiv$ is an equivalence relation, which has the following properties:

1. $(r, s) \equiv (r, s)$
2. $(r, s) \equiv (r_1, s_1)$ iff $(r_1, s_1) \equiv (r, s)$
3. If $(r, s) \equiv (r_1, s_1)$ and $(r_1, s_1) \equiv (r_2, s_2)$, then $(r, s) \equiv (r_2, s_2)$

where $r, r_1, r_2 \in R$ and $s, s_1, s_2 \in D$. Motivated by the case $R = \mathbb{Z}$, we now define a fraction $\frac{r}{s}$ to be the equivalence class $[(r, s)]$ of the pair (r, s) in X. Let F denote the set of all these fractions:

$$F = \left\{ \frac{r}{s} : r \in R, s \in D \right\} = \left\{ \frac{r}{s} : r, s \in R, s \neq 0 \right\}.$$

The addition and multiplication on F are defined

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1} \text{ and } \frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where $r, r_1 \in R$ and $s, s_1 \in D$. Note that $ss_1 \neq 0$ since R is an integral domain. Hence, these operations are well-defined. As an exercise, one can show that with the above definition of addition and multiplication, F becomes a field with zero $\frac{0}{1}$, unity $\frac{1}{1}$, and the negative of $\frac{r}{s}$ being $\frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0$ in F, $r \neq 0$ and thus $\frac{s}{r} \in F$ and we have

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs} = \frac{1}{1} \in F.$$

In addition, $R \cong R'$ where

$$R' = \left\{ \frac{r}{1} : r \in R \right\} \subseteq F.$$

Thus, we have

Theorem 9.8 Let R be an integral domain. Then there exists a field F consisting of fractions $\frac{r}{s}$ with $r, s \in R$ and $s \neq 0$. By identifying $r = \frac{r}{1}$ for all $r \in R$, we can view R as a subring of F. Such F is called the field of fractions of R.

Remark: Given integral domain R, one can generalize the above set $D = R \backslash \{0\}$ to any subset $D \subseteq R$ satisfying

1. $0 \notin D$
2. $1 \in D$
3. If $a, b \in D$, then $ab \in D$.

Then one can show that the corresponding set of fractions F is an integral domain containing R. Such F is called the ring of fractions of R over D and is denoted $D^{-1}R$.

Remark 2: If R is an integral domain and P is a prime ideal, take $D = R \backslash P$. Then D satisfies conditions 1-3 above. The resulting $D^{-1}R$ is called the localization of R at the prime ideal P.

Section 10

Polynomial Rings

Subsection 10.1

Polynomials over Rings

Let R be a ring and x be a variable. Let

$$R[x] = \{f(x) : a_0 + a_1x + ... + a_{m-1}x^{m-1} + a_mx^m : m \in \mathbb{N} \cup \{0\}, a_i \in R\}.$$

Such $f(x)$ is called a polynomial in x over R. If $a_m \neq 0$, we say $f(x)$ has degree m, denoted $\deg f = m$, and we say a_m is the leading coefficient of $f(x)$.

If the leading coefficient is 1, we say $f(x)$ is monic. If $\deg f = 0$, then $f(x) = a_0 \in R\backslash\{0\}$. In this case, we say $f(x)$ is a constant polynomial.

Note that

$$f(x) = 0 \iff a_0 = a_1 = ... = 0.$$

We define $\deg 0 = -\infty$ and will see why we use this convention later this chapter. Note that $f(x) = 0$ is also a constant polynomial.

Let

$$f(x) = a_0 + ... + a_mx^m \in R[x]$$
$$g(x) = b_0 + ... + b_nx^n \in R[x]$$

with $m \neq n$. Then, we write $a_i = 0$ for all $m + 1 \leq i \leq n$. We define addition and multiplication on $R[x]$ as follows:

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n \\ f(x)g(x) &= (a_0 + ... + a_mx^m)(b_0 + ... + b_nx^n) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_1 + a_1b_1 + a_0b_2)x^2 + ... + a_mb_nx^{m+n} \\ &= c_0 + c_1x + ... + c_{m+n}x^{m+n} \end{aligned}$$

where

$$c_i = a_0b_i + a_1b_{i-1} + ... + a_{i-1}b_1 + a_ib_0.$$

Then, one can show that under these operations

Proposition 10.1 Let R be a ring and x be a variable. Then

1. $R[x]$ is a ring
2. R is a subring of $R[x]$
3. If $Z = Z(R)$ is the center of R, then $Z(R[x]) = Z[x]$

1. Exercise
2. R is the same as the set of constant polynomials
3. Let $f(x) = a_0 + a_1x + ... + a_mx^m \in Z[x]$ and $g(x) = b_0 + b_1x + ... + b_nx^n \in R[x]$. Then
$$f(x)g(x) = c_0 + c_1x + ... + c_{m+n}x^{m+n}$$

Week 11.1

where $c_i = a_0b_i + ... + a_ib_0$. Thus, $f(x)g(x) = g(x)f(x)$ since $a_i \in Z(R)$ for all $0 \leq i \leq m$, so $Z[x] \subseteq Z(R[x])$.

To show the other inclusion, if $f(x) = a_0 + ... + a_mx^m \in Z(R[x])$, then $f(x)b = bf(x)$ for all $b \in R \subseteq R[x]$. It follows that $a_ib = ba_i$ for all $0 \leq i \leq m$ meaning $a_i \in Z$ and so $Z(R[x]) \subseteq Z[x]$.

Warning: Although $f(x) \in R[x]$ can be used to define a function from R to R, the polynomial is not the same as the function it defines. For example, if $R = \mathbb{Z}_2$, then $\mathbb{Z}_2[x]$ is an infinite set, but there are only four distinct functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.

Proposition 10.2 Let R be an integral domain. Then

1. $R[x]$ is an integral domain
2. If $f(x) \neq 0$ and $g(x) \neq 0$ in $R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$
3. The units in $R[x]$ are R^*, the units in R

Proof We will prove (1) and (2) together. Suppose $f(x) \neq 0$ and $g(x) \neq 0$ in $R[x]$ where $f(x) = a_0 + ... + a_mx^m$ and $g(x) = b_0 + ... + b_nx^n$ where $a_m, b_n \neq 0$. Then,

$$f(x)g(x) = (a_mb_n)x^{m+n} + ... + a_0b_0.$$

Since R is an integral domain, $a_mb_n \neq 0$ and so $f(x)g(x) \neq 0$. So, $R[x]$ is also an integral domain, and $\deg(fg) = m + n = \deg(f) + \deg(g)$.

For (3), let $u(x) \in R[x]$ be a unit with inverse $v(x)$. Since $u(x)v(x) = 1$, by (2) we have $\deg(u) + \deg(v) = \deg(1) = 0$. Since $u(x)v(x) = 1$, $u(x) \neq 0$ and $v(x) \neq 0$. Since $\deg(u) \geq 0$ and $\deg(v) \geq 0$, $\deg(u) = 0 = \deg(v)$. Thus, u and v are units in R and $R[x]^* \subseteq R^*$. Since $R^* \subseteq R[x]^*$, then $R^* = R[x]^*$. □

Remark 1: Note that in $\mathbb{Z}_4[x]$, $2x \cdot 2x = 4x^2 = 0$. Thus, $\deg(2x) + \deg(2x) \neq \deg(2x \cdot 2x)$. Hence, the product formula only applies when the ring is an integral domain.

Remark 2: To extend the product formula to 0, we define $\deg(0) = \pm\infty$.

Subsection 10.2

Polynomials over a Field

In this section, we will consider $F[x]$ where F is a field and explore its analogies with the set of integers $\mathbb{Z}$.

Definition 10.1 (Divisibility of Polynomials) Let F be a field and $f(x), g(x) \in F[x]$. We say $f(x)$ divides $g(x)$, denoted $f(x)|g(x)$, if there exists $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$.

Proposition 10.3 Let F be a field and $f(x), g(x), h(x) \in F[x]$. Then

1. If $f(x)|g(x)$ and $g(x)|h(x)$, then $f(x)|h(x)$
2. If $f(x)|g(x)$ and $f(x)|h(x)$, then $f(x)|(g(x)u(x) + h(x)v(x))$ for any $u(x), v(x) \in F[x]$

Proposition 10.4 Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials. If $f(x)|g(x)$ and $g(x)|f(x)$, then $f(x) = g(x)$.

Proof Since $f(x)|g(x)$ and $g(x)|f(x)$, $g(x) = r(x)f(x)$ and $f(x) = s(x)g(x)$ for some $r(x), s(x) \in F[x]$. Then $f(x) = r(x)s(x)f(x)$. By Proposition 10.2, Week 11.2

$$\deg(f) = \deg(r) + \deg(s) + \deg(f)$$

so $\deg(s) = \deg(r) = 0$. Thus $f(x) = sg(x)$ for some $s \in F$. Since both $f(x)$ and $g(x)$ are monic, $s = 1$ so $f(x) = g(x)$. □

Proposition 10.5 (Division Algorithm) Let F be a field and $f(x), g(x) \in F[x]$ where $f(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that

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

with $\deg(r) < \deg(f)$. Note that this includes the case for $r = 0$.

Proof We first prove by induction that such $q(x)$ and $r(x)$ exist. Write $m = \deg(f)$ and $n = \deg(g)$. If $n < m$, then $g(x) = 0f(x) + g(x)$. So, suppose $n \geq m$ and the result holds for all $g \in F[x]$ with $\deg(g) < n$. Write $f(x) = a_0 + ... + a_m x^m$ where $a_m \neq 0$ and $g(x) = b_0 + ... + b_n x^n$ where $b_n \neq 0$. Since F is a field, a_m^{-1} exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^1 x^{n-m} f(x) \\ &= b_n x^n + ... + b_0 - b_n a_m^{-1} x^{n-m}(a_m x^m + ... + a_0) \\ &= 0x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1})x^{n-1} + ... \end{aligned}$$

Since $\deg(g_1) < n$, by induction, there exist $q_1(x), r_1(x) \in F[x]$ where $g_1(x) = q_1(x)f(x) + r_1(x)$ where $\deg(r_1) < \deg(f)$. It follows that

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x)f(x) + r_1(x)) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x) + b_n a_m^{-1} x^{n-m})f(x) + r_1(x) \end{aligned}$$

By taking $q(x) = q_1(x) + b_n a_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$, the result follows. To prove uniqueness, suppose we also have $g(x) = q_1(x)f(x) + r_1(x)$ where $\deg(r_1) < \deg(f)$. Then

$$r(x) - r_1(x) = (q_1(x) - q(x))f(x)$$

If $q_1(x) - q(x) \neq 0$, then we get $\deg(r - r_1) = \deg(q_1 - q) + \deg(f) \geq \deg(f)$ leading to contradiction since $\deg(r - r_1) < \deg(f)$. Thus, $q_1(x) - q(x) = 0$ and $r(x) - r_1(x) = 0$. □

Proposition 10.6 Let F be a field and $f(x), g(x) \in F[x]$ where $f(x), g(x) \neq 0$. Then there exist $d(x) \in F[x]$ satisfying

1. $d(x)$ is monic
2. $d(x)|f(x)$ and $d(x)|g(x)$
3. If $e(x)|f(x)$ and $e(x)|g(x)$, $e(x)|d(x)$
4. $d(x) = u(x)f(x) + v(x)g(x)$ for some $u(x), v(x) \in F[x]$

Note that if both $d(x)$ and $d_1(x)$ satisfy the above, since $d(x)|d_1(x)$ and $d_1(x)|d(x)$ and both are monic, then $d(x) = d_1(x)$ by Proposition 10.4. We call such $d(x)$ the greatest common divisor of $f(x)$ and $g(x)$, denoted

$$d(x) = \gcd(f(x), g(x)).$$

Proof Consider the set $X = \{u(x)f(x) + v(x)g(x) : u(x), v(x) \in F[x]\}$. Since $f(x) \in X$, the set contains nonzero polynomials and thus contains monic polynomials (since F is a field, if $h(x) \in X$ with leading coefficient a, then $a^{-1}h(x) \in X$ and is monic). Among all monic polynomials in X, choose $d(x) = u(x)f(x) + v(x)g(x)$ of minimal degree. Then (1), (4) are satisfied. For (3), if $e(x)|f(x)$ and $e(x)|g(x)$, since $d(x) = u(x)f(x)+v(x)g(x)$, then by Prop 10.3, $e(x)|d(x)$. It remains to prove (2).

By division algorithm, write $f(x) = q(x)d(x) + r(x)$ where $\deg(R) < \deg(d)$. Then Week 11.3

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)(u(x)f(x) + v(x)g(x)) \\ &= (1 - q(x)u(x))f(x) - (q(x)v(x))g(x) \end{aligned}$$

Note that if $r(x) \neq 0$, write $c \neq 0$ to be the leading coefficient of $r(x)$. Since F is a field, $c^{-1} \in F$ exists. The above expression of $r(x)$ shows that $c^{-1}r(x)$ is a monic polynomial of X with $\deg(c^{-1}r) = \deg(r) < \deg(d)$ which contradicts the minimality of $\deg(d)$. So, we must have $r(x) = 0$ and so $d(x)|f(x)$. Similarly, we can show $d(x)|g(x)$. □

We recall $p \in \mathbb{Z}$ is prime if $p \geq 2$ and whenever $p = ab$ where $a, b \in \mathbb{Z}$, $a = \pm 1$ or $b = \pm 1$. Note that ± 1 are units of $\mathbb{Z}$.

Definition 10.2 (Irreducible Polynomial) If F is a field, a polynomial $\ell(x) \neq 0$ in $F[x]$ is irreducible if $\deg(\ell) \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ in $F[x]$, we have $\deg(\ell_1) = 0$ or $\deg(\ell_2) = 0$ where degree 0 polynomials are the units in $F[x]$.

If a polynomial is not irreducible, we say it is reducible.

Example If $\ell(x) \in F[x]$ satisfies $\deg(\ell) = 1$, then $\ell(x)$ is irreducible.

Example One can show that if $\deg(f) = 2$ or $\deg(f) = 3$, then f is irreducible iff $f(d) \neq 0$ for any $d \in F$.

Example Let $\ell(x), f(x) \in F[x]$. If $\ell(x)$ is irreducible and $\ell(x) \nmid f(x)$, then $\gcd(\ell(x), f(x)) = 1$.

Proposition 10.7 Let F be a field and $f(x), g(x) \in F[x]$. If $\ell(x) \in F[x]$ is irreducible and $\ell(x)|f(x)g(x)$, then $\ell(x)|f(x)$ or $\ell(x)|g(x)$.

Proof Suppose $\ell(x)|f(x)g(x)$. We have two cases.

1. If $\ell(x)|f(x)$, we are done.
2. If $\ell(x) \nmid f(x)$, then $d(x) = \gcd(\ell(x), f(x)) = 1$. By Proposition 10.6, $1 = \ell(x)u(x) + f(x)v(x)$ for some $u(x), v(x) \in F[x]$. Then

$$g(x) = g(x)\ell(x)u(x) + g(x)f(x)v(x).$$

Since $\ell(x)|\ell(x)$ and $\ell(x)|g(x)f(x)$, by Proposition 10.3, we have $\ell(x)|g(x)$.

□

Remark: Let $f_1(x), ..., f_n(x) \in F[x]$ and let $\ell(x) \in F[x]$ be irreducible. If $\ell(x)|f_1(x)...f_n(x)$, by applying Proposition 10.7 repeatedly, we get $\ell(x) \mid f_i(x)$ for some $1 \leq i \leq n$.

Theorem 10.8 (Unique Factorization Theorem) Let F be a field and let $f(x) \in F[x]$ where $\deg(f) \geq 1$. Then we can write

$$f(x) = c\ell_1(x)\ell_2(x)...\ell_m(x)$$

where $c \in F^*$ and $\ell_i(x)$ are monic, irreducible polynomials. This factorization is unique up to the order of ℓ_i.

Example One can prove using Theorem 10.8 that there are infinitely many irreducible polynomials in $F[x]$.

Proposition 10.9 Let F be a field. Then all ideals of $F[x]$ are of the form

$$\langle h(x)\rangle = h(x)F[x]$$

for some $h(x) \in F[x]$. If $\langle h(x)\rangle \neq 0$ and $h(x)$ is monic, then the generator is uniquely determined.

Week 12.1

Proof Let A be an ideal of $F[x]$. If $A = \{0\}$ then $A = \langle 0\rangle$. If $A \neq \{0\}$, then we know A contains a monic polynomial. This is because since F is a field, then if $f \in A$ with a leading coefficient a, then $a^{-1}f \in F$ as well.

Among all monic polynomials in A, choose $h(x) \in A$ of minimal degree. Then $\langle h(x)\rangle \subseteq A$. To show the other inclusion, let $f(x) \in A$. By division algorithm, we can write $f(x) = q(x)h(x) + r(x)$ where $\deg(r) < \deg(h)$. If $r(x) \neq 0$, let $u \neq 0$ be its leading coefficient. Since A is an ideal, $f(x), h(x) \in A$ and we have

$$u^{-1}r(x) = u^{-1}(f(x) - q(x)h(x)) = u^{-1}f(x) - u^{-1}q(x)h(x) \in A$$

which is a monic polynomial in A with $\deg(u^{-1}r) < \deg(h)$. This is a contradiction, so $r(x) = 0$ and $f(x) = q(x)h(x)$, implying $f(x) \in \langle h(x)\rangle$ and so $A = \langle h(x)\rangle$. □

Let $A \neq 0$ be an ideal of $F[x]$. By Proposition 10.9, we can write $A = \langle h(x)\rangle$ for a unique monic polynomial $h(x) \in F[x]$. Suppose $\deg(h) = m \geq 1$. Consider the quotient ring $R = F[x]/A$ and thus

$$R = \{\bar{f}(x) = f(x) + A : f(x) \in F[x]\}.$$

Write $t = \bar{x} = x + A$. Then by division algorithm, we can show

$$R = \{\bar{a_0} + \bar{a_1}t + ... + \bar{a}_{m-1}t^{m-1} : a_i \in F\}.$$

Consider the map $\theta : F \to R$ given by $\theta(a) = \bar{a}$. Since θ is not the zero map and $\ker\theta$ is an ideal of F, we have $\ker\theta = \{0\}$ since F only has two ideals $\{0\}$ and F. Thus, θ is a one-to-one ring homomorphism. Since $F \cong \theta(F)$, identifying F with $\theta(F)$, we can write

$$R = \{a_0 + a_1t + ... + a_{m-1}t^{m-1} : a_i \in F, h(t) = 0\}.$$

Note in R, we have (ex)

$$a_0 + ... + a_{m-1}t^{m-1} = b_0 + ... + b_{m-1}t^{m-1} \iff a_i = b_i, 0 \leq i \leq m-1.$$

Theorem 10.10 Let F be a field and $h(x) \in F[x]$ be a monic polynomial where $\deg(h) = m \geq 1$. Then the quotient ring $R = F[x]/\langle h(x)\rangle$ is given by

$$R = \{a_0 + a_1 t + ... + a_{m-1}t^{m-1} : a_i \in F, h(t) = 0\}$$

in which an element of R can be uniquely determined in the above form.

Example In $\mathbb{Z}$, when we divide an integer by $n \in \mathbb{N}$, the remainder is $0 \leq r < n$. Thus, we have

$$\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle = \{[0], ..., [n-1]\} = \{0 + \langle n\rangle, ..., (n-1) + \langle n\rangle\}.$$

Example Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By Proposition 10.10,

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{a + bt : a, b \in \mathbb{R}, t^2 + 1 = 0\} \cong \{a + bi : a, b \in \mathbb{R} : i^2 = -1\} \cong \mathbb{C}$$

We recall $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ is a field (or integral domain) iff n is prime.

Proposition 10.11 Let F be a field and $h(x) \in F[x]$ with $\deg(h) \geq 1$. The following are equivalent:

1. $F[x]/\langle h(x)\rangle$ is a field
2. $F[x]/\langle h(x)\rangle$ is an integral domain
3. $h(x)$ is irreducible in $F[x]$

Example Consider $x^3 + x + 1$ in $\mathbb{Z}_2$. Since $x = 0$ and $x = 1$ are not roots of $x^3 + x + 1$, the polynomial is irreducible. Thus

$$\mathbb{Z}_2/\langle x^3 + x + 1\rangle = \{a + bt + ct^2 : a, b, c \in \mathbb{Z}_2 \text{ and } t^3 + t + 1 = 0\}$$

is a field of 8 elements.

Example Since $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ is a field, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

Example Since $x^2 + x + 1$ has no root in $\mathbb{Z}_2$, it is irreducible in $\mathbb{Z}_2[x]$. Thus $\mathbb{Z}_2[x]$ is a field of 4 elements $\mathbb{F}_4$. Note that $\mathbb{F}_4$ is not the same as $\mathbb{Z}_4$.

We will now prove Proposition 10.11. Week 12.2

Proof Let $A = \langle h(x)\rangle$.

(1) $\implies$ (2). Every field is an integral domain.

(2) $\implies$ (3). Suppose for the sake of contradiction that $h(x)$ is reducible, so $h(x) = f(x)g(x)$ where $f(x), g(x) \in F[x]$. Then

$$(f(x) + A)(g(x) + A) = f(x)g(x) + A = h(x) + A = 0 + A \in F[x]/A.$$

By (2), either $f(x)+A = 0+A$ or $g(x)+A = 0+A$. If $f(x) \in A$, then $f(x) = q(x)h(x)$ for some $q(x) \in F[x]$. Then $h(x) = f(x)g(x) = q(x)h(x)g(x)$. Since $F[x]$ is an integral domain, this implies that $q(x)g(x) = 1$ which gives $\deg(g) = 0$. Similarly, if $g(x) \in A$, then we get $\deg(f) = 0$. This contradicts the definition of reducibility, so $h(x)$ is irreducible in $F[x]$.

(3) $\implies$ (1). Note that $F[x]/A$ is a commutative ring. Thus, to show that it is a field. it suffices to show that every non-zero element in $F[x]/A$ has an inverse. Let $f(x) + A \neq 0 + A$ where $f(x) \in F[x]$. Then $f(x) \notin A$ and hence $h(x) \not| f(x)$.

Since $h(x)$ is irreducible and $h(x) \not| f(x)$, then $\gcd(h(x), f(x)) = 1$. By Proposition 10.6, there exist $u(x), v(x) \in F[x]$ such that

$$1 = u(x)f(x) + v(x)h(x).$$

Thus $(u(x) + A)(f(x) + A) = 1 + A$ since $h(x) \in A$ so

$$(h(x) + A)(v(x) + A) = (0 + A)(v(x) + A) = 0 + A.$$

It follows that $f(x) + A$ has an inverse in $F[x]/A$ and hence $F[x]/\langle h(x)\rangle$ is a field. □

Example We can make the following analogies between $\mathbb{Z}$ and $F[x]$ where F is a field:

	$\mathbb{Z}$	$F[x]$
Elements	m	$f(x)$
Size	$\lvert m\rvert$	$\deg(f)$
Units	$\{\pm 1\}$	$F^* = F\backslash\{0\}$
Positives	$\mathbb{Z}\backslash\{0\} = \pm\mathbb{N}$	$F[x]\backslash\{0\} = F^* \cdot \{h : h \text{ is monic}\}$
Unique Factorization	$m = \pm 1 p_1^{\alpha_1} ... p_r^{\alpha_r}$, p_i prime	$f(x) = c\ell_1^{\alpha_1} ... \ell_r^{\alpha_r}$, $c \in F^*$, ℓ_i monic, irreducible
Ideals	$\langle n\rangle$ (unique if $n \in \mathbb{N}$)	$\langle h(x)\rangle$ (unique if $h(x)$ monic)
Quotient Rings	$\mathbb{Z}/\langle n\rangle$ is a field iff n prime	$F[x]/\langle h(x)\rangle$ is a field iff $h(x)$ irreducible

End of Test 2 Material

Subsection 10.3

Fermat's Last Theorem in $F[x]$

We recall that Fermat's Last Theorem states for $n \geq 3$, the equation $x^n + y^n = z^n$ has no non-trivial solution in $\mathbb{Z}$. Trivial solutions are assignments of 1's and 0's like $(x, y, z) = (1, 0, 1)$.

Now, we consider the same theorem over polynomial fields. Let F be a field and $n \in \mathbb{N}$ where $n \geq 3$. Consider the equation

$$f(x)^n + g(x)^n = h(x)^n$$

where $f(x), g(x), h(x) \in F[x]$. We say (f, g, h) is non-trivial if $\deg(f), \deg(g), \deg(h) \geq 1$. Also, we say a solution (f, g, h) is coprime if $\gcd(f(x), g(x)) = \gcd(f(x), h(x)) = \gcd(g(x), h(x)) = 1$.

Proposition 10.12 Let F be a field with $\mathrm{ch}(F) = 0$ and $n \in \mathbb{N}$ with $n \geq 3$. There is no non-trivial coprime solution for the equation

$$f(x)^n + g(x)^n = h(x)^n$$

where $f(x), g(x), h(x) \in F[x]$.

Proof Suppose we have a non-trivial coprime solution. Without loss of generality, suppose $\deg(f) = \deg(h) \geq \max(\deg(g), 1)$. Let us write $f'(x) = \frac{df}{dx}$. Since $f^n + g^n = h^n$, we can take derivatives to get

$$nf^{n-1}f' + ng^{n-1}g' = nh^{n-1}h'.$$

Since $\mathrm{ch}(F) = 0$ and $n \neq 0$, multiplying both sides by h gives

$$f^{n-1}f'h + g^{n-1}g'h = h^n h' = f^n h' + g^n h'.$$

It follows that

$$f^{n-1}(f'h - fh') = g^{n-1}(gh' - g'h).$$

Since $\gcd(f, g) = 1$, we have $f^{n-1} | (gh' - g'h)$. Thus,

$$(n-1)\deg(f) \leq \deg(g) + \deg(h) - 1.$$

Since we said $\deg(f) = \deg(h) \geq \deg(g)$ earlier,

$$(n-2)\deg(f) \leq \deg(g) - 1.$$

This is a contradiction for $n \geq 3$. Therefore, there is no non-trivial coprime solution for (f, g, h). □

Subsection 10.4

Prime Number Theorem and The Riemann Hypothesis

We define $\pi(x) = \#\{p \leq x : p \text{ prime}\}$. Week 12.3

Theorem 10.13 (Conjecture of Gauss) $\pi(x) \sim \mathrm{li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$

The conjecture of Gauss states that the probability that a number less than or equal to x is prime is $\frac{1}{\log x}$. For example, for $n \in \mathbb{N}$ with $1 \leq n \leq e^{100}$, about 1% are prime.

Definition 10.3 (Riemann Zeta Function) For $s \in \mathbb{C}$, the Riemann zeta function is defined to be

$$\begin{aligned}\zeta(s) &= \sum_{n \in \mathbb{N}} \frac{1}{n^s} \\ &= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \\ &= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right)\end{aligned}$$

One can show that $\zeta(s)$ converges absolutely for $\mathrm{Re}(s) > 1$ and $\zeta(s)$ can be extended to the whole $\mathbb{C}$.

Theorem 10.14 (Riemann Hypothesis) There is no nontrivial zero of $\zeta(s)$ for $\mathrm{Re}(s) > \frac{1}{2}$.

Theorem 10.15 (Prime Number Theorem (Hadamard, de la Vallée Poussin)) For any $n \in \mathbb{N}$,

$$\pi(x) = \mathrm{li}(x) + o\left(\frac{x}{(\log x)^n}\right)$$

Assuming the Riemann Hypothesis, we can show that $\pi(x) = \mathrm{li}(x) + o(x^{1/2+\epsilon})$ for any $\epsilon > 0$. Let us consider now the prime number theorem over $\mathbb{Z}_p[x]$. For $f(x) \in \mathbb{Z}_p[x]$, we

define $|f(x)| = p^{\deg f}$. For $s \in \mathbb{C}$, the zeta function of $\mathbb{Z}_p[t]$ is

$$\zeta_p(s) = \sum_{f \text{ monic}} \frac{1}{|f|^s} = \prod_{\ell \text{ monic irreducible}} \left(1 - \frac{1}{|\ell|^s}\right)^{-1}.$$

Observe that $\#\{f : \text{monic}, \deg(f) = d\} = p^d$. Hence

$$\zeta_p(s) = \sum_{d=0}^{\infty} \frac{p^d}{p^{ds}} = \sum_{d=0}^{\infty} (p^{1-s})^d = \frac{1}{1-p^{1-s}}.$$

Then

$$\pi_p(x) = \#\{\ell : \text{monic, irreducible}, |\ell| \leq x\} = \frac{p}{p-1} \frac{x}{\log_p x} + o(x^{1/2+\epsilon})$$

for any $\epsilon > 0$, so the Riemann hypothesis holds in $\mathbb{Z}_p[x]$.

This leads us to the question: are problems in $\mathbb{Z}[x]$ always easier than in $\mathbb{Z}$? The answer is no: as an example, we will show that Taylor series do not work in $\mathbb{Z}_p[x]$.

For $F[x] \in \mathbb{Z}[x]$ and $\in \mathbb{Z}$, we write the Taylor polynomial

$$F(x) = \sum_{i=0}^{\infty} a_i (x-a)^i \text{ where } a_i = \frac{F^{(i)}(a)}{i!}.$$

Let $G_x(t) \in (\mathbb{Z}_p[x])[t]$. For $b \in \mathbb{Z}_p[x]$, one may consider to write

$$G_x(t) = \sum_{i=0}^{\infty} b_i (t-b)^i \text{ where } b_i = \frac{G_x^{(i)}(b)}{i!}.$$

If $\deg(G_x) \geq p$, we know at least one of the $b_i(x-b)^i$ terms should be non-zero if $i \geq p$. However, also note that if $i \geq p$,

$$i! = 1 \times 2 \times 3 \times ... \times p \times (p+1) \times ... \times i.$$

Since $i!$ is divisible by p, we have $i! = 0$. This is a contradiction, thus b_i is not well defined.