Contents

09/07, lecture 1-1

Chapter 1 Groups

1.1 Notation

Notation. Number Notation: We use the following conventions:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$
- $\mathbb{R}$ = real numbers
- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$.
- $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ is the integers modulo n for $n \in \mathbb{N}$ and where $[r]$ is the congruence class given by $\{z \in \mathbb{Z} : z \equiv r \pmod{n}\}$ for $0 \leq r \leq n-1$.

Notation. Matrix Notation: For $n \in \mathbb{N}$, an $n \times n$ matrix over a field is a $n \times n$ array

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

We denote $\mathsf{M}_n(\mathbb{F})$ the set of $n \times n$ matrices over $\mathbb{F}$. Recall the usual matrix operations.

1.2 Groups

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

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

Proposition 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. If e_1 and e_2 are identities, then $e = e_1 \star e_2 = e_2$.

2. If b_1 and b_2 are inverses of a, then

$$b_1 = b_1 \star e = b_1 \star (a \star b_2) = (b_1 \star a) \star b_2 = e \star b_2 = b_2 \qquad \square$$

Definition. Abelian Group: A group G is said to be abelian if $a \star b = b \star a$ for all $a, b \in G$. I.e., if the group operation is commutative.

Example: The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups with identity 0 and the inverse of a given by $-a$. However, $(\mathbb{N}, +)$ is not a group since there is no identity nor inverses. Similarly, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are not groups since 0 has no inverse.

Notation: For a set S, let S^* denote the subset of S containing only elements with multiplicative inverses.

Example: With the above notation we have $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. And so $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are abelian groups with identity 1 and the inverse of r given by $\frac{1}{r}$.

09/09, lecture 1-2

Remark: To show e is an identity of G, it suffices to show that $e \star a = a$ for all $a \in G$. Similarly to show b is an inverse of a it suffices to show $a \star b = e$.

Example: The set $(\mathsf{M}_n(\mathbb{R}), +)$ is an abelian group with identity $\mathcal{O}$ (the zero matrix) and the inverse of $A = [a_{ij}]$ is given by $-A = [-a_{ij}]$.

Example: The set $(\mathsf{M}_n(\mathbb{R}), \cdot)$ has identity I_n (the identity matrix), but not all matrices have inverse so $\mathsf{M}_n(\mathbb{R})$ is not a group.

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

Remark: Note if $A, B \in GL_n(\mathbb{R})$, then $\det(A \cdot B) = \det(A) \cdot \det(B) \neq 0$, so $GL_n(\mathbb{R})$ is closed under $\cdot$. Furthermore, we know matrix multiplication is associative (MATH 146). Note the identity I_n has $\det(I_n) = 1 \neq 0$, so $I_n \in GL_n(\mathbb{R})$. Finally note since all $M \in GL_n(\mathbb{R})$ have $\det(M) \neq 0$, we know M has an inverse M^{-1} and that $\det(M^{-1}) \neq 0$. Therefore, we see that $GL_n(\mathbb{R})$ is a group. However, since not all matrices commute $GL_n(\mathbb{R})$ is not abelian for $n \geq 2$.

Definition. Direct Product: Let $(G, \star_G)$ and $(H, \star_H)$ be groups. Their direct product is the set $G \times H$ with the component-wise group operation $\star$ given by

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2).$$

Note: Note for any groups G and H, the direct product $G \times H$ is a group. In particular it has identity $(1_G, 1_H)$ 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 $G_1, \ldots, G_n$ are groups, then $G_1 \times \cdot \times G_n$ is a group.

Notation: Given a group G and $g_1, g_2 \in G$, we often denote the identity of G by 1 and $g_1 \star g_2$ by $g_1 g_2$. Further, since the inverse is unique we often denote the inverse of $g \in G$ by g^{-1}.

Notation: Let G be a group and $g \in G$. We write $g^0 = 1$ and for $n \in \mathbb{N}$ we write

$$g^n = \underbrace{g \star \cdots \star g}_{n \text{ times}} \qquad \text{and} \qquad g^{-n} = \underbrace{g^{-1} \star \cdots \star g^{-1}}_{n \text{ times}}$$

Proposition 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. $g^n g^m = g^{n+m}$.
4. $(g^n)^m = g^{nm}$.

Proof.

1. Recall the inverse is unique and note $g^{-1} g = 1$ by definition, so g is the inverse of g^{-1}, as desired.
2. Note
$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1g^{-1} = gg^{-1} = 1$$
3. Can be shown by induction on m.
4. Can be shown by induction on m. □

Note: **Warning:** It is **not** generally true that if $gh \in G$ then $(gh)^n = g^n h^n$.

Example: Note $(gh)^2 = ghgh$, but $g^2 h^2 = gghh$. Thus $(gh)^2 = g^2 h^2$ if and only if $gh = hg$.

Proposition 3: Let G be a group and $g, h, f \in G$ and $a, b \in G$. Then

1. They satisfy left and right cancellation. That is (1-a) if $gh = gf$, then $h = f$ and (1-b) if $hg = fg$ then $h = f$.
2. The equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.

Proof.

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

1.3 Symmetric Groups

Definition. 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.

Example: Let $L = \{1, 2, 3\}$. Then S_L has the following permutations:

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

Where each element maps to the element below it. E.g., for the last permutation listed above, denoted σ, $\sigma(1) = 3$, $\sigma(2) = 2$, and $\sigma(3) = 1$.

Definition. Symmetric Group: For $n \in \mathbb{N}$ we define $S_n = S_{\{1,\ldots,n\}}$ to be the set of all permutations of $\{1, \ldots, n\}$ and we call it the symmetric group of order n.

Proposition 4: $|S_n| = n!$.

Proof. Let $\sigma \in S_n$. There are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, ..., 2 choices for $\sigma(n-1)$, and 1 choice $\sigma(n)$. $\square$

09/12, lecture 2-1

Note: Given $\sigma, \tau \in S_n$, we can compose them to create another permutation $\sigma\tau$ given by $\sigma\tau(x) = \sigma(\tau(x))$. Further, since σ and τ are bijections, so is $\sigma\tau$.

Example: Compute $\sigma\tau$ and $\tau\sigma$ given

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

Note $\sigma\tau(1) = \sigma(2) = 4$ and $\sigma\tau(2) = \sigma(4) = 2$. Continuing in this manner we find

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

Note then that $\sigma\tau \neq \tau\sigma$.

Exploration: Note if $\sigma, \tau, \mu \in S_n$, then $\sigma(\tau\mu) = (\sigma\tau)\mu$ by the associativity of composition. Note also the identity is $\varepsilon \in S_n$ given by

$$\varepsilon = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

So for all $\sigma \in S_n$, $\sigma\varepsilon = \sigma = \varepsilon\sigma$. Finally, for $\sigma \in S_n$, since σ is a bijection, it has a unique inverse bijection $\sigma^{-1} \in S_n$ called the inverse permutation. This permutation is such that $\sigma(\sigma^{-1}(x)) = x = \sigma^{-1}(\sigma(x))$ for all $x \in \{1, \ldots, n\}$. That is, $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$.

Example: Find σ^{-1} for

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

Since $\sigma(1) = 4$, we have $\sigma^{-1}(4) = 1$. Continuing in this manner we have

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

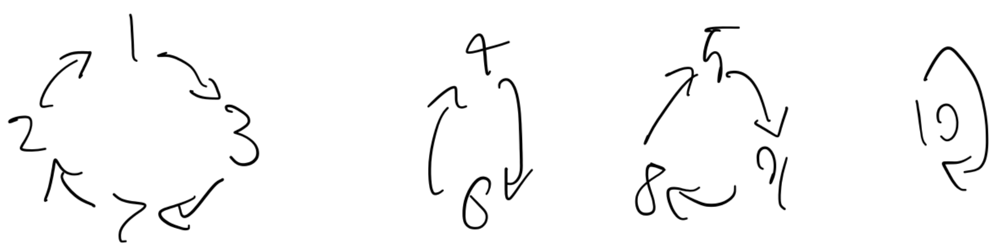
Proposition 5: S_n is a group.

Proof. See the above exploration. □

Remark: Consider

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

Writing it in this form is inconvenient as we have to write the numbers 1 through 10 twice. Note that $\sigma(1) = 3$, $\sigma(3) = 7$, $\sigma(7) = 2$, and $\sigma(2) = 1$, this forms a cycle.



Thus σ can be decomposed as a 4-cycle $(1\ 3\ 7\ 2)$, a 3-cycle $(5\ 9\ 8)$, a 2-cycle $(4\ 6)$, and a 1-cycle (10), though we don't usually write 1-cycles. Note these cycles are disjoint. Note also we have

$$\begin{aligned} \sigma &= (1\ 3\ 7\ 2)(4\ 6)(5\ 9\ 8) \\ &= (4\ 6)(5\ 9\ 8)(1\ 3\ 7\ 2) \\ &= (6\ 4)(9\ 8\ 5)(7\ 2\ 1\ 3) \end{aligned}$$

Theorem 6. Cycle Decomposition Theorem: Let $\sigma \in S_n$ with $\sigma \neq \varepsilon$. Then σ is the product of (one or more) disjoint cycles of length at least 2. The factorization is unique up to the ordering of the factors.

Proof. See A1 bonus. □

Remark: By convention, we consider every permutation in S_n as also being a permutation in S_{n+1} by fixing the mapping of $n+1$. Thus $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq S_{n+1} \subseteq \cdots$.

1.4 Cayley Tables

Definition. Cayley Table: For a finite group G, we may define its operation by means of a table. 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 a Cayley table.

Remark: By cancellation, the entries in each row and column of the Cayley table is unique.

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

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

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

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

Remark: In the above example, if we replace 1 by $[0]$ and -1 by $[1]$ then the Cayley tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are the same. In this case we say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are **isomorphic** and write $\mathbb{Z}^* \cong \mathbb{Z}_2$.

Definition. Cyclic Group: For $n \in \mathbb{N}$, the cyclic group of order n is defined by $C_n = \{1, a, a^2, \dots, a^{n-1}\}$ with $a^n = 1$ and where $a^i \neq a^j$ for all $i, j \in \{0, \dots, n-1\}$ with $i \neq j$. We may also write $C_n = \langle a : a^n = 1 \rangle$; this is called the generator of C_n.

Remark: The Cayley Table of C_n is

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

09/14, lecture 2-2

Proposition 7: Let G be a group. Up to isomorphism we have

1. If $|G| = 1$, then $G \cong \{1\}$.
2. If $|G| = 2$, then $G \cong C_2$.
3. If $|G| = 3$, then $G \cong C_3$.
4. If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$ where K_4 is the Klein 4-group.

Proof. 1. Obvious

2. If $|G| = 2$, then $G = \{1, g\}$ with $g \neq 1$. We know that $1 \star 1 = 1$ and $1 \star g = g = g \star 1$. Note that if $g \star g = g$, then g must be the identity, i.e., $g = 1$, a contradiction. Hence $g \star g = 1$. Thus the Cayley Table is

G	1	g
1	1	g
g	g	1

which is exactly the Cayley table of of C_2. We see then that $G = \langle g : g^2 = 1 \rangle \cong C_2$.

3. If $|G| = 3$, then $G = \{1, g, h\}$ with $g \neq 1$, $h \neq 1$, $g \neq h$. We can begin filling in the Cayley table for rows and columns corresponding to 1. If $gh = g$ or $gh = h$, then $h = 1$ or $g = 1$ by cancellation, respectively, which is a contradiction since $g \neq 1$ and $h \neq 1$. So $gh = 1 = hg$. Finally, since all entries in a given row or column must be distinct, we must have $g^2 = h$ and $h^2 = g$. The Cayley table is thus

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

The Cayley table for C_3 is noted below

C_3	1	a	a^2
1	1	a	2^2
a	a	a^2	1
a^2	a^2	1	a

By identifying $g \mapsto a$ and $h \mapsto a^2$, we see the above two tables are the same. Thus if $|G| = 3$, then $G \cong C_3$.

4. See A1. $\square$

Chapter 2 Subgroups

2.1 Subgroups

Definition. Subgroup: Let G be a group and $H \subseteq G$ be a subset of G. If H itself is a group, then we say that H is a subgroup of G.

Note. Subgroup Test: Since G is a group, for $h_1, h_2, h_3 \in H \subseteq G$, we have $h_1(h_2h_3) = (h_1h_2)h_3$. Thus H is a subgroup if it satisfies the following conditions.

1. If $h_1, h_2 \in H$, then $h_1h_2 \in H$.

2. $1_G \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Example: Given a group G, then $\{1\}$ and G are subgroups of G.

Example: We have a chain of groups $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$.

Example. Special Linear Group: Recall the general linear group of order n over $\mathbb{R}$ is

$$GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot) = \{M \in \mathsf{M}_n(\mathbb{R}) : \det(M) \neq 0\}.$$

Define

$$SL_n(\mathbb{R}) = (SL_n(\mathbb{R}), \cdot) = \{M \in \mathsf{M}_n(\mathbb{R}) : \det(M) = 1\} \subseteq GL_n(\mathbb{R}).$$

Note that the identity $I \in SL_n(\mathbb{R})$. If $A, B \in SL_n(\mathbb{R})$, then

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1.$$

Further, we have

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1.$$

Thus $AB, A^{-1} \in SL_n(\mathbb{R})$. By the subgroup test, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. We call $SL_n(\mathbb{R})$ the special linear group of order n over $\mathbb{R}$.

Example. Center of Group: Given a group G, we define the center of G to be

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}$$

That is $Z(G)$ is the set of elements that commute with all other elements. Note $Z(G) = G$ if G is abelian. We claim $Z(G)$ is an abelian subgorup of G.

Proof. Note that $1_G \in Z(G)$ since the identity commutes. Let $y, z \in Z(G)$. Then for all $g \in G$ we have

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

since $z, y \in Z(G)$, thus we see $zy \in G$ since it commutes with any $g \in G$. Since $z \in Z(G)$, for all $g \in G$ we have $zg = gz$. Then by multiplying by z^{-1} we have

$$\begin{aligned} zg &= gz \\ z^{-1}(zg)z^{-1} &= z^{-1}(gz)z^{-1} \\ (z^{-1}z)gz^{-1} &= z^{-1}g(zz^{-1}) \\ gz^{-1} &= z^{-1}g \end{aligned}$$

Thus we see that $z^{-1} \in Z(G)$. So by the subgroup test we see that $Z(G)$ is a subgroup of G. We also see that clearly $Z(G)$ is abelian by definition, as desired. □

Proposition 8: Let H and K be subgroups of a group G. Then their intersection

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

is also a subgroup of G.

Proof. Note since H and K are subgroups of G, we have $1_G \in H$ and $1_G \in K$, thus $1_G \in H \cap K$. Let $g, h \in H \cap K$. Then note $gh \in H$ and $gh \in K$ since each is a (closed) subgroup, then $gh \in H \cap K$. Finally note since $g \in H$ and $g \in K$ we have $g^{-1} \in H$ and $g^{-1} \in K$, thus $g^{-1} \in H \cap K$. So by the subgroup test $H \cap K$ is a subgroup of G. □

Proposition 9. Finite Subgroup Test: If H is a finite nonempty set of a group G, then H is a subgroup of G if and only if H is closed under its operation.

Proof. ($\Longrightarrow$) This is obvious.

($\Longleftarrow$) For $H \neq \emptyset$, let $h \in H$. Since H is closed under its operation, $h, h^2, h^3, \ldots$ are all in H. Since H is finite, these elements cannot all be distinct. Thus $h^n = h^{n+m}$ for some $n, m \in \mathbb{N}$. By cancellation, this implies $h^m = 1$. Also, we have $h^{-1} = h^{m-1}$. Thus by the subgroup test H is a subgroup (since it contains the identity and its inverses). □

09/16, lecture 2-3

2.2 Alternating Groups

Definition. Transposition: A transposition $\sigma \in S_n$ is a cycle of length 2, i.e., $\sigma = (a\ b)$ with $a, b \in \{1, \ldots, n\}$ and $a \neq b$.

Example: Consider the permutation $(1\ 2\ 4\ 5)$. Also the composition $(1\ 2)(2\ 4)(4\ 5)$ can be computed as

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

where after the first row you apply $(4\ 5)$, after the second row you apply $(2\ 4)$, and after the third you apply $(1\ 2)$. Thus we have that $(1\ 2\ 4\ 5) = (1\ 2)(2\ 4)(4\ 5)$. We can also show that $(1\ 2\ 4\ 5) = (2\ 3)(1\ 2)(2\ 5)(1\ 3)(2\ 4)$. Thus we see that the decomposition of a permutation into transpositions is not unique.

Theorem 10. Parity Theorem: If a permutation σ has two factorization $\sigma = \gamma_1\gamma_2 \cdots \gamma_r = \mu_1\mu_2 \cdots \mu_s$ where each γ_i and μ_j is a transposition, then $r \equiv s \pmod 2$ (i.e., r and s have the same parity).

Proof. See bonus 2. □

Definition. Even/odd permutation: A permutation σ is even (resp. odd) if it can be written as a product of an even (resp. odd) number of transpositions. By the parity theorem, a permutation is either even or odd, but not both.

Theorem 11. Alternating Group: For $n \geq 2$, let A_n denote the set of all even permutations in S_n. Then

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

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

Proof. 1. $\varepsilon = (1\ 2)(2\ 1) \in A_n$.

2. If $\sigma, \tau \in A_n$, we can write $\sigma = \sigma_1 \cdots \sigma_r$ and $\tau = \tau_1 \cdots \tau_s$ where σ_i, τ_j are transpositions, and r and s are even integers. Then
$$\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$$
is a product of $(r + s)$ transpositions, and thus $\sigma\tau$ is even. Also we note that since σ_i is a transposition, we have $\sigma_i^2 = \varepsilon$, and thus $\sigma_i^{-1} = \sigma_i$. It follows that
$$\sigma^{-1} = (\sigma_1\sigma_2 \cdots \sigma_r)^{-1} = \sigma_r^{-1}\sigma_{r-1}^{-1} \cdots \sigma_1^{-1} = \sigma_r\sigma_{r-1} \cdots \sigma_1$$

3. Let O_n denote the set of all odd permutations in S_n. Then $S_n = A_n \cup O_n$ and the parity implies $A_n \cap O_n = \emptyset$. Since $|S_n| = n!$ and $|S_n| = |A_n| + |O_n|$, to prove $|A_n| = \frac{1}{2}n!$, it suffices to show that $|A_n| = |O_n|$. Define
$$f : A_n \to O_n \qquad \sigma \mapsto (1\ 2)\sigma.$$
Since σ is even, $(1\ 2)\sigma \in O_n$, thus the map is well-defined. Note if σ_1, σ_2 are such that
$$f(\sigma_1) = (1\ 2)\sigma_1 = (1\ 2)\sigma_2 = f(\sigma_2)$$
then by cancellation $\sigma_1 = \sigma_2$, so f is injective. Finally, if $\tau \in O_n$, then $\sigma = (1\ 2)\tau \in A_n$. Also
$$f(\sigma) = (1\ 2)(1\ 2)\tau = \tau,$$
thus f is surjective. It follows then that f is a bijection, and so $|A_n| = |O_n|$ and $|A_n| = \frac{1}{2}n!$. □

2.3 Order of Elements

Definition. Generated Cyclic Groups: Let G be a group and $g \in G$. We call $\langle g \rangle := \{g^k : k \in \mathbb{Z}\}$ the <u>cyclic subgroup of G generated by g</u>. If $G = \langle g \rangle$ for some $g \in G$, then we say G is a cyclic group and g is a generator of G.

Proposition 12: If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Proof. Note that $1 = g^0 \in \langle g \rangle$. Also, if we $x = g^m \in \langle g \rangle$ and $y = g^n \in \langle g \rangle$, then $xy = g^m g^n = g^{m+n} \in \langle g \rangle$, and $x^{-1} = g^{-m} \in \langle g \rangle$. So by the subgroup test, $\langle g \rangle$ is a subgroup of G. □

Example: Consider $(\mathbb{Z},+)$. Note for all $k \in \mathbb{Z}$, we can write $k = k \cdot 1$ and $k \cdot 1 = 1^k$ in our group. Thus $(\mathbb{Z},+) = \langle 1 \rangle$. Similarly we can show $(\mathbb{Z},+) = \langle -1 \rangle$. We observe that for any $n \in \mathbb{Z}$ with $n \neq \pm 1$, there exists no $k \in \mathbb{Z}$ such that $kn = 1$. Thus ± 1 are the only generators of $(\mathbb{Z},+)$.

09/19, lecture 3-1

Remark: Let G be a group and $g \in G$. Suppose that there exists $k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k = 1$. Then $g^{-k} = (g^k)^{-1} = 1^{-1} = 1$. Thus we can assume $k \geq 1$. Then by the well-ordering principle, there exists the 'smallest' positive integer n such that $g^n = 1$.

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

Proposition 13: Let G be a group and $g \in G$ be such that $o(g) = n \in \mathbb{N}$. Let $k \in \mathbb{Z}$. Then

1. $g^k = 1$ if and only if $n \mid k$.
2. $g^k = g^m$ if and only if $k \equiv m \pmod{n}$.
3. $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ where $1, g, g^2, \ldots, g^{n-1}$ are all distinct.

Proof.

1. ($\implies$) Note by the division algorithm we can write $k = qn + r$ for some $q \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Then we have
$$1 = g^k = g^{qn}g^r = (g^n)^q g^r = g^r$$
But n is the smallest positive integer such that $g^n = 1$ and $r < n$, so $r = 0$. Then $k = qn$ and so $n \mid k$.
($\impliedby$) If $n \mid k$, then $k = nq$ for some $q \in \mathbb{Z}$. Thus
$$g^k = g^{nq} = (g^n)^q = 1^q = 1$$
2. Note $g^k = g^m$ if and only if $g^{k-m} = 1$. This is true if and only if $n \mid (k-m)$ by (1), which is equivalent to $k \equiv m \pmod{n}$.
3. By (2), the elements of $\{1, g, g^2, \ldots, g^{n-1}\}$ are all distinct, as $0 \leq i, j \leq n-1$ have $i \equiv j \pmod{n}$ if and only if $i = j$. We see clearly that $\{1, g, \ldots, g^{n-1}\} \subseteq \langle g \rangle$ by definition. To prove the other inclusion, let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Then by the division algorithm we can write $k = qn + r$ for $q \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Then
$$x = g^k = g^{nq+r} = (g^n)^q g^r = 1 \cdot g^r = g^r \in \{1, g, g^2, \ldots, g^{n-1}\}$$
since $0 \leq r \leq n-1$. □

Proposition 14: Let G be a group and $g \in G$ be such that $o(g) = \infty$. Let $k \in \mathbb{Z}$. Then

1. $g^k = 1$ if and only if $k = 0$.
2. $g^k = g^m$ if and only if $k = m$.
3. $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g^1, g^2, \ldots\}$ where all g^i are distinct.

Proof. 1. ($\implies$) Suppose $g^k = 1$ and by way of contradiction suppose $k \neq 0$. Then $g^{-k} = (g^k)^{-1} = 1$, so we can assume $k \geq 1$. But then $o(g) \leq k < \infty$, a contradiction. Thus we need that $k = 0$.

   ($\impliedby$) Obviously $g^0 = 1$.

2. Note $g^k = g^m$ if and only if $g^{k-m} = 1$. By (1), this is true if and only if $k - m = 0$ or $k = m$.

3. Let $i, j \in \mathbb{Z}$. Then $g^i = g^j$ if and only if $i = j$ by (2), so all elements of $\langle g \rangle$ are distinct. □

Proposition 15: Let G be a group and $g \in G$ be such that $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$ with $d \mid n$, then $o(g^d) = \frac{n}{d}$.

Proof. Write $k = \frac{n}{d}$. Note that $(g^d)^k = g^{dk} = g^n = 1$. Thus it remains to show k is the smallest such positive integer. Suppose $(g^d)^r = 1$ with $r \in \mathbb{N}$. Then $g^{dr}{=}1$. Since $o(g) = n$, by a previous proposition, we have $n \mid dr$. Thus there is a $q \in \mathbb{Z}$ such that $dr = nq = (dk)q$. Since $d \neq 0$, we have $r = kq$. Note that r and k are positive integers, so if $r = kq$ we must have that q is a positive integer. Hence $r = kq \geq k \cdot 1 = k$, thus $o(g^d) = k = \frac{n}{d}$. □

2.4 Cyclic Groups

Remark: Recall that if a group $G = \langle g \rangle$ for some $g \in G$, then G is a cyclic group.

Proposition 16: Every cyclic group is abelian.

Proof. Let $G = \langle g \rangle$ for some $g \in G$. Note that if $a, b \in G$, then we have $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$. Then note

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba.$$

It follows then that every cyclic group is abelian. □

Remark: Note the converse of the above proposition is not true. For instance, the Klein 4-group $K_4 \cong C_2 \times C_2$ is abelian, but K_4 is not cyclic.

Proposition 17: Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle g \rangle$ and $H \subseteq G$ be a subgroup. If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic. If $H \neq \{1\}$, then there is $g^k \in H$ with $k \in \mathbb{Z}$ and $k \neq 0$. Since H is a group, we have $g^{-k} \in H$, thus we can assume $k \geq 1$. Let m be the smallest positive integer such that $g^m \in H$. Then we claim $H = \langle g^m \rangle$.

Notice since H is a group and $g^m \in H$, we clearly have that $\langle g^m \rangle \subseteq H$, it remains to show the other inclusion. By way of contradiction, suppose there is some $g^k \in H$ with $g^k \notin \langle g^m \rangle$ for $k \in \mathbb{Z}$. Then clearly $m \nmid k$ as otherwise $g^k \in \langle g^m \rangle$. Then by the division algorithm, there is a $q \in \mathbb{Z}$ and $0 < r < m$ (note $r \neq 0$ since $m \nmid k$) with $k = qm + r$. But since H is a group $g^k g^{-qm} = g^r \in H$. This is a contradiction since $0 < r < m$ but m was assumed to be the smallest positive integer with $g^m \in H$. Thus $H \subseteq \langle g^m \rangle$. □

09/21, lecture 3-2

Proposition 18: 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 $\gcd(k, n) = 1$.

Proof. ($\Longleftarrow$) If $\gcd(k, n) = 1$, by Euclid's Lemma there exists $x, y \in \mathbb{Z}$ such that $1 = kx + ny$. Thus

$$g = g^1 = g^{kx+ny} = (g^k)^x (g^n)^y = (g^k)^x \in g^k$$

Then we see that $G = \langle g \rangle = \langle g^k \rangle$ since $g \in \langle g^k \rangle$.

($\Longrightarrow$) If $G = \langle g^k \rangle$, then $g \in \langle g^k \rangle$. Thus there exists $x \in \mathbb{Z}$ such that $g = g^{kx}$, i.e., $1 = g^{kx-1}$. Since $o(g) = n$, by proposition 13, we have $n \mid (kx - 1)$. Thus there exists $y \in \mathbb{Z}$ such that $kx - 1 = ny$, or equivalently $1 = kx - ny$. Since $1 \mid k$ and $1 \mid n$ and $1 = kx - ny$, by the GCD characterization theorem (see MATH 135), we have $\gcd(k, n) = 1$. □

Remark: If $G = \langle g \rangle$ with $o(g) = n \in \mathbb{N}$, then $o(g^k) = \frac{n}{\gcd(n,k)}$. We can prove this with a similar argument to proposition 15.

Theorem 19. Fundamental Theorem of Finite Cyclic Groups: Let $G = \langle g \rangle$ be a cyclic group of order n. Then

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

Proof. 1. By proposition 17, H is cyclic, so $H = \langle g^m \rangle$ for some $m \in \mathbb{N}$. Let $d = \gcd(m, n)$. Then we claim $H = \langle g^d \rangle$.

Since $d \mid m$, we have $m = dk$ for some $k \in \mathbb{Z}$. Then

$$g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle$$

Thus we have $H = \langle g^m \rangle \subseteq \langle g^d \rangle$. To prove the other inclusion, since $d = \gcd(m, n)$, by Euclid's Lemma there exists $x, y \in \mathbb{Z}$ such that $d = mx + ny$. Then

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

Thus $\langle g^d \rangle \subseteq \langle g^m \rangle$. It follows that $H = \langle g^d \rangle$. By proposition 13 and 15, we have $|H| = o(g^d) = \frac{n}{d}$, thus $|H| \mid n$.

2. Note that $\langle g^{n/k} \rangle$ is a subgroup of G with order k. Let K be a subgroup of G which is of order k with $k \mid n$. By (1), let $K = \langle g^d \rangle$ with $d \mid n$. Then by proposition 13 and 15, we have $k = |K| = o(g^d) = \frac{n}{d}$. It follows that $d = \frac{n}{k}$. And thus $K = \langle g^{n/k} \rangle$. □

2.5 Non-cyclic Groups

Definition. Generating Sets: Let X be a nonempty subset of a group G. Let

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

denote the set of all products of powers of (not necessarily distinct) elements of X. Then $\langle X \rangle$ is a subgroup of G containing X, called the subgroup of G generated by X.

Example: The Klein 4-group $K_4 = \{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$ and $ab = c$ (or $ac = b$ or $bc = a$). Thus $K_4 = \langle a, b : a^2 = 1 = b^2, ab = ba \rangle$. We can also replace a, b by a, c or b, c.

Example: The symmetric group of degree 3, $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$. One can take cycles $\sigma = (1, 2, 3)$ and $\tau = (1, 2)$. Thus

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

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

Definition. Dihedral Group: For $n \geq 2$, the dihedral group of order $2n$ is defined by

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

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 $D_6 \cong S_3$. In general, for $n \geq 3$, D_{2n} is the group of symmetries of a regular n-gon (a = rotation of $\frac{2\pi}{n}$ radians and b = reflection through x-axis).

09/23, lecture 3-3

Chapter 3 Normal Subgroups

3.1 Homomorphisms and Isomorphisms

Definition. Group Homomorphism: Let G and H be groups. A mapping $\alpha : G \to H$ is a group homomorphism if $\alpha(a \star_G b) = \alpha(a) \star_H \alpha(b)$ for all $a, b \in G$. We often write $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$.

Example: Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ given by $A \mapsto \det(A)$. Given that $\det(AB) = \det(A)\det(B)$, we have that the mapping is a homomorphism.

Proposition 20: 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 $g \in G$ and $k \in \mathbb{Z}$.

Proof.

1. Note that $1_H\alpha(1_G) = 1_H\alpha(1_G^2) = 1_H\alpha(1_G)^2$ thus by cancelling $1_H\alpha(1_G)$ we see that $\alpha(1_G) = 1_H$.
2. Note that $\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1_G) = 1_H$ by (1), thus $\alpha(g)^{-1} = \alpha(g^{-1})$.
3. The case that $k = 0$ follows by (1), it follows for $k \geq 1$ by induction. The case that $k < 0$ follows by (2). □

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

Proposition 21:

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

Proof. See A3. □

Remark: Note that $\cong$ defines an equivalence relation. In particular, from the above we have from (1) $G \cong G$, from (2) if $G \cong H$ then $H \cong G$, and from (3) if $G \cong H$ and $H \cong K$, then $G \cong K$.

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

Proof. Define $\sigma : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ by $\sigma(r) = e^r$. Note $\sigma = \exp$ is invertible, and thus is a bijection. Also for $r, s \in \mathbb{R}$ we have

$$\sigma(r + s) = e^{r+s} = e^r \cdot e^s = \sigma(r) \cdot \sigma(s)$$

Thus σ is also a homomorphism, and so σ is an isomorphism. □

Example: We claim $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^*, \cdot)$.

Proof. By way of contradiction, suppose that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. Then τ is onto, and so there exists $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Then we have

$$2 = \tau(q) = \tau\left(\frac{q}{2} + \frac{q}{2}\right) = \tau\left(\frac{q}{2}\right) \cdot \tau\left(\frac{q}{2}\right) = \tau\left(\frac{q}{2}\right)^2.$$

So $\tau\left(\frac{q}{2}\right) = \sqrt{2} \notin \mathbb{Q}^*$. Then τ is not well-defined, a contradiction. We see then that $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$. □

3.2 Cosets and Lagrange's Theorem

Definition. Coset: Let H be a subgroup of a group G. If $a \in G$, we define

$$Ha = \{ha : h \in H\}$$

to be the right coset of H generated by a. Similarly, we define

$$aH = \{ah : h \in H\}$$

to be the left coset of H generated by a.

Remark: Note that $H1 = H = 1H$. Note also that $a \in Ha$ and $a \in aH$. Moveover, notice that if $h_1 a \in Ha$ and $h_2 a \in Ha$, it is not necessarily true that $(h_1 a)(h_2 a) = h_3 a$ for some $h_3 \in H$, and so cosets are not necessarily a group. However, note that if if H is abelian, then we have $Ha = aH$ for all $a \in G$.

Example: let $K_4 = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ab = ba$. Let $H = \{1, a\}$. Note since K_4 is abelian we have $gH = Hg$ for all $g \in K_4$. Thus the (right or left) cosets of H are $H1 = \{1, a\} = Ha$ and $Hb = \{b, ab\} = Hab$. Thus there are exactly two cosets of H in K_4.

Example: Let $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau, \tau\sigma^2\}$ with $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau\sigma = \tau$. Let $H = \{\varepsilon, \tau\}$. Since $\sigma\tau = \tau\sigma^2$, the right cosets of H are

$$\begin{aligned} H\varepsilon &= \{\varepsilon, \tau\} = H\tau \\ H\sigma &= \{\sigma, \tau, \sigma\} = H\tau\sigma \\ H\sigma^2 &= \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2 \end{aligned}$$

Also, the left cosets of H are

$$\begin{aligned} \varepsilon H &= \{\varepsilon, \tau\} = \tau H \\ \sigma H &= \{\sigma, \tau\sigma^2\} = \tau\sigma^2 \\ \sigma^2 H &= \{\sigma^2, \tau\sigma\} = \tau\sigma H \end{aligned}$$

Note that $H\sigma \neq \sigma H$ and $H\sigma^2 \neq \sigma^2 H$.

09/26, lecture 4-1

Proposition 22: Let H be a subgroup of a group G, and let $a, b \in G$. Then

1. $Ha = Hb$ if and only if $ab^{-1} \in H$. In particular, we have $Ha = H$ if and only if $a \in H$.
2. If $a \in Hb$, then $Ha = Hb$.
3. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Thus the distinct right cosets of H form a partition of G.

Proof. 1. ($\Longrightarrow$) If $Ha = Hb$, then $a = 1a \in Ha = Hb$. Thus $a = hb$ for some $h \in H$, and we have then $ab^{-1} = h \in H$.

($\Longleftarrow$) Suppose $ab^{-1} \in H$. Then for all $h \in H$, we have $ha = h(ab^{-1})b \in Hb$ since $h(ab^{-1}) \in H$. Thus $Ha \subseteq Hb$. Since H is a group and $ab^{-1} \in H$, we have $(ab^{-1}) = ba^{-1} \in H$. Thus for all $h \in H$, we have $hb = h(ba^{-1})a \in Ha$ since $h(ba^{-1}) \in H$. Thus $Hb \subseteq Ha$, and so $Ha = Hb$, as desired.

2. If $a \in Hb$, then $ab^{-1} \in H$. Thus by (1), $Ha = Hb$.

3. If $Ha \cap Hb \neq \emptyset$, then there exists $x \in Ha \cap Hb$. Since $x \in Ha$, by (2) we have $Ha = Hx$. Similarly $Hb = Hx$. Thus we have $Ha = Hx = Hb$. □

Remark: The analogue of proposition 22 also holds for left cosets. For (1), $aH = bH$ if and only if $b^{-1}a \in H$.

Definition. Index of a Group: By proposition 22, we see that G can be written as a disjoint union of right cosets of $H \subseteq G$. We define the index $[G : H]$ to be the number of distinct right cosets of H in G.

Theorem 23. Lagrange's Theorem: Let H be a subgroup of a finite group G. We have $|H| \mid |G|$ and $[G : H] = \frac{|G|}{|H|}$.

Proof. Write $k = [G : H]$. Let $Ha_1, Ha_2, \ldots, Ha_k$ be the set of distinct right cosets of H in G. By proposition 22, $G = Ha_1 \cup Ha_2 \cup \cdots Ha_k$ is a disjoint union (since $Ha_i \cap Ha_j = \emptyset$ for all $i \neq j$, and so the union of all distinct right cosets is exactly G). Note that

$$|Ha_i| = |\{ha_i : h \in H\}| = |H|.$$

So we have

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_k| = k|H|$$

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

Corollary 24: Let G be a finite group and let $g \in G$. Then

1. $o(g) \mid |G|$.
2. If $|G| = n$, then $g^n = 1$.

Proof. 1. Take $H = \langle g \rangle$ in theorem 23. Note that we have then $|H| = o(g)$. So by theorem 23 we have $o(g) = |H| \mid |G|$.

2. Let $o(g) = m$. Then by (1) we have $m \mid n$. Thus
$$g^n = (g^m)^{n/m} = 1^{n/m} = 1. \qquad \square$$

Remark. Fermat's Little Theorem: Let $\mathbb{Z}_n^*$ be the set of invertible elements in $\mathbb{Z}_n$. Thus
$$\mathbb{Z}_n^* = \big\{k \in \{0, 1, 2, \dots, n-1\} : \gcd(k, n) = 1\big\}.$$
Define the Euler φ-function, $\varphi(n)$, to be the order of $\mathbb{Z}_n^*$. I.e.,
$$\varphi(n) = |\mathbb{Z}_n^*| = \left|\big\{k \in \{0, 1, 2, \dots, n-1\} : \gcd(k, n) = 1\big\}\right|.$$
As a direct consequence of corollary 24 (2), we see that $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then we have $a^{\varphi(n)} \equiv 1 \pmod n$ since $|\mathbb{Z}_n^*|$ is a group with $|\mathbb{Z}_n^*| = \varphi(n)$. Note that if $n = p$ for some prime p, then $\varphi(p) = p - 1$. Thus we have if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$. This provides a very short and simple proof of Fermat's Little Theorem.

Corollary 25: If G is a group with $|G| = p$, for some prime p. Then $G \cong C_p$ where C_p is the cyclic group of order p.

Proof. Let $g \in G$ with $g \neq 1$. By corollary 24, we have $o(g) \mid p$. Since $g \neq 1$ and p is a prime, we have $o(g) > 1$ and so $o(g) = p$ as 1 and p are the only divisors of p. By proposition 13, $|\langle g\rangle| = o(g) = p$. It follows that $G = \langle g\rangle \cong C_p$. $\square$

Corollary 26: Let H and K be finite subgroup of G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof. We have proved in proposition 8 that $H \cap K$ is a subgroup of both H and K. By Lagrange's Theorem, $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. It follows that $|H \cap K| \mid \gcd(|H|, |K|)$. I.e., $|H \cap K| \mid 1$, and so $H \cap K$ is a group (note then that $1 \in H \cap K$) with $|H \cap K| = 1$, and thus necessarily $H \cap K = \{1\}$. $\square$

09/28, lecture 4-2

3.3 Normal Subgroups

Definition. Normal Subgroups: Let H be a subgroup of a group G. If $gH = Hg$ for all $g \in G$, then we say H is <u>normal</u> in G, denoted by $H \lhd G$.

Example: We have $\{1\} \lhd G$ and $G \lhd G$ for all groups 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 definition we have $Z(G) \lhd G$. Thus every subgroup of $Z(G)$ is normal in G.

Example: If G is an abelian group, then every subgroup of G is normal in G. However, the converse of this statement is false. See, for instance, the quaternion group in question 8 of A3.

Proposition 27. Normality Test: Let H be a subgroup of a group G. The following statements are equivalent:

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

Proof. ($1 \implies 2$) Let $x \in gHg^{-1}$, say $x = ghg^{-1}$ for some $h \in H$. Then by (1) $gh \in gH = Hg$ (since $H \lhd G$). Say $gh = h_1 g$ for some $h_1 \in H$. Then

$$x = ghg^{-1} = h_1 gg^{-1} = h_1 \in H$$

So we see $gHg^{-1} \subseteq H$.

($2 \implies 3$) If $g \in G$, then by (2) $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g in (2), we get $g^{-1}Hg \subseteq H$. This implies that $H \subseteq gHg^{-1}$ by multiplying both sides by g^{-1} and g. Thus from (2) since $gHg^{-1} \subseteq H$, we have $gHg^{-1} = H$.

($3 \implies 1$) If $gHg^{-1} = H$ for all $g \in G$, then $gH = Hg$ for all $g \in G$ by multiplying both sides by g on the right. Thus $H \lhd G$. $\square$

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

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

Thus $ABA^{-1} \in H$ and it follows that $AHA^{-1} \subseteq H$ for all $A \in G$. By the normality test, we have $H \lhd G$., i.e., $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Proposition 28: If H is a subgroup of a group G and $[G : H] = 2$, then $H \lhd G$.

Proof. Let $a \in G$. If $a \in H$, then $Ha = H = aH$. If $a \notin H$, since $[G : H] = 2$, then $G = H \cup Ha$ and this union is disjoint. Thus $Ha = G \setminus H$. Similarly, $aH = G \setminus H$ as necessarily $aH \neq H$. Thus $Ha = aH$ for all $a \in G$, i.e., $H \lhd G$. $\square$

Example: Let A_n be the alternating group contained in S_n. Since $[S_n : A_n] = 2$ (multiplying by an even permutation is the same, multiplying by an odd permutation creates exactly one distinct coset of permutations of odd length), by proposition 28 $A_n \lhd S_n$ where A_n is the alternating group of order n.

Example: Let

$$D_{2n} = \langle a, b | a^n = 1 = b^2, \text{ and } aba = b\rangle = \{1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$$

be the dihedral group of order $2n$. Since $[D_{2n} : \langle a\rangle] = 2$ ($a\langle a\rangle = \langle a\rangle = \langle a\rangle a$ and $b\langle a\rangle = \langle a\rangle b$), by proposition 28, we have $\langle a\rangle \triangleleft D_{2n}$.

Remark. Group Product: Let H and K be subgroups of a group G. Their intersection $H \cap K$ is the "largest" subgroup of G contained in both H and K. One may wonder if there is a "smallest" subgroup of G containing both H and K. Note that $H \cup K$ is the "smallest" subset containing H and K. However, one can show that $H \cup K$ is a subgroup only if $H \subseteq K$ or $K \subseteq H$ (see Piazza). A more useful construction turns out to be the product HK of H and K defined as

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

Note that $H \subseteq HK$ and $K \subseteq HK$ since we can take one of h or k to be 1. Note, however, HK is not always a group, and in particular HK is not necessarily closed.

Lemma 29: Let H and K be subgroups of a group G. The following are equivalent.

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

Proof. We will prove ($1 \iff 2$) and then ($2 \iff 3$) follows by interchanging H and K.

($1 \implies 2$) Let $kh \in KH$ with $k \in K$ and $h \in H$. Since H and K are subgroups of G we have $k^{-1} \in K$ and $h^{-1} \in H$. Since HK is also a subgroup of G, we have $h^{-1}k^{-1} \in HK$ and thus $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus we have $KH \subseteq HK$.

Similarly, let $hk \in HK$ with $h \in H$ and $k \in K$. Since H and K are subgroups of G we have $h^{-1} \in H$ and $k^{-1} \in K$. Since HK is also a subgroup of G we have $k^{-1}h^{-1} = (hk)^{-1} \in HK$ and thus $(hk)^{-1} \in KH$, however, this implies $hk = ((hk)^{-1})^{-1} \in KH$. Thus we have $HK \subseteq KH$, and so $HK = KH$.

($2 \implies 1$) We have $1 = 1 \cdot 1 \in HK$. Also if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Also for $h_1k_1, h_2k_2 \in HK$, we have $k_1h_2 \in KH = HK$, say $k_1h_2 = h_3k_3$. It follows that

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK.$$

By the subgroup test, HK is a subgroup of G. □

09/30, lecture 4-3

Proposition 30: Let H and K be subgroups of a group G. Then

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

Proof. 1. Suppose $H \lhd G$. Then since $gH = Hg$ for all $g \in G$ (since $H \lhd G$), we have

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH.$$

Then by lemma 29, $HK = KH$ is a subgroup of G.

2. Let $g \in G$ and $hk \in HK$. Since $H \lhd G$ and $K \lhd G$, we have

$$g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

since $g^{-1}Hg = H$ and $g^{-1}Kg = K$. Thus $HG \lhd G$. □

Definition. Normalizer: Let H be a subgroup of G. The normalizer of H denoted by $N_G(H)$ is defined to be

$$N_G(H) = \{g \in G : gH = Hg\}$$

Note $H \lhd G$ if and only if $N_G(H) = G$.

Note: Note that in the proof of proposition 30 (1), we do not need the full assumption that $H \lhd G$. We only need that $kH = Hk$ for all $k \in K$, or equivalently that $K \subseteq N_G(H)$.

Corollary 31: Let H and K be subgroups of a group G. If $K \subseteq N_G(H)$, then $KH = HK$ is a subgroup of G.

Proof. See the above note and the proof of proposition 30 (1). □

Theorem 32: Let H and K be subgroups of a group G. If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

Proof. Claim 1: If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. To see this, consider $x = hkh^{-1}k^{-1}$. We will show that $x = 1$, and then since h and k are arbitrary, we will see that $hk = kh$. Note that $hkh^{-1} \in K$ since $K \lhd G$, and necessarily $k^{-1} \in K$. So $x = (hkh^{-1})k \in K$. Similarly, note that $kh^{-1}k^{-1} \in H$ since $H \lhd G$, and necessarily $h \in H$. So $x = h(kh^{-1}k^{-1}) \in H$. Then since $x \in H \cap K$, we see $x = 1$, and thus $hk = kh$.

Since $H \lhd G$, by proposition 30, HK is a subgroup of G. Define

$$\sigma : H \times K \to HK, \qquad (h, k) \mapsto hk$$

Claim 2: σ is an isomorphism. To see this, note first that σ is well-defined, though we omit a proof. Let $(h_1, k_1), (h_2, k_2) \in H \times K$. By claim 1, we have $h_2k_1 = k_1h_2$. Thus,

$$\sigma((h_1, k_1)(h_2, k_2)) = \sigma((h_1h_2, k_1k_2)) = (h_1h_2)(k_1k_2) = (h_1k_1)(h_2k_2) = \sigma((h_1, k_1))\sigma((h_2, k_2)),$$

so we see that σ is a homomorphism. Note that by the definition of HK, σ is also surjective (since all $x \in HK$ is the product of $h \in H$ and $k \in K$, thus $\sigma((h, k)) = x$). Also, if $\sigma((h_1, k_1)) = \sigma((h_2, k_2))$, we have $h_1k_1 = h_2k_2$. Thus $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$. Thus $h_1 = h_2$ and $k_1 = k_2$, i.e., σ is injective. Thus σ is an isomorphism, and so claim 2 holds, i.e., $HK \cong H \times K$. □

Corollary 33: Let H and K be subgroups of a finite group G. If $H \triangleleft G$ and $K \triangleleft G$ satisfy $H \cap K = \{1\}$ and $|H| \cdot |K| = |G|$, then $G \cong H \times K$.

Proof. By theorem 32, $|HK| = |H| \cdot |K| = |G|$ and since HK is a subgroup of G, we see that necessarily $G \cong HK \cong H \times K$. □

Example: Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Let G be a cyclic group of order mn. Write $G = \langle a \rangle$ with $o(a) = mn$. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$ so that $|H| = o(a^n) = m$ and $|K| = o(a^m) = n$. It follows that $|H| \cdot |K| = |G|$. Since $\gcd(m, n) = 1$, by corollary 26 $H \cap K = \{1\}$. Thus by corollary 33, we have

$$G \cong H \times K \cong C_m \times C_n$$

Chapter 4 Isomorphism Theorems

4.1 Quotient Groups

Remark: Let K be a subgroup of a group G. Consider the set of right cosets of K, i.e., $\{Ka : a \in G\}$. Can we make $\{Ka : a \in G\}$ to become a group? A natural way to define the group operation (or multiplication) on this set is

$$(Ka)(Kb) = K(ab) \qquad \forall a, b \in G \tag{*}$$

Note that we could have $Ka_1 = Ka_2$ and $Kb_1 = Kb_2$ with $a_1 \neq a_2$ and $b_1 \neq b_2$. Thus in order for (*) to make sense, a necessary condition is

$$Ka_1 = Ka_2 \quad \text{and} \quad Kb_1 = Kb_2 \quad \implies \quad Ka_1b_1 = Ka_2b_2$$

In this sense, we mean that the group operation $KaKb = Kab$ is well-defined.

Lemma 34: Let K be a subgroup of a group G. The following are equivalent:

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

10/03, lecture 5-1

Proof. (2 $\implies$ 1) Let $a \in G$ and $k \in K$ be arbitrary. To show $K \triangleleft G$, it is sufficient to show $aka^{-1} \in K$. Since $Ka = Ka$ and $Kk = K1$, then by (2) we have $Kak = Ka1$, i.e., that $Kak = Ka$. In particular, we see then that $Kaka^{-1} = K$, however, this is the case if and only if $aka^{-1} \in K$, as desired.

(1 $\implies$ 2) Let $Ka_1 = Ka_2$ and $Kb_1 = Kb_2$. Then we see that $Ka_1a_2^{-1} = K$ and $Kb_1b_2^{-1}$, but again, this is the case if and only if $a_1a_2^{-1} \in K$ and $b_1b_2^{-1} \in K$. Moreover, since K is a

group, $(a_1a_2^{-1})^{-1} = a_2a_1^{-1} \in K$ and $(b_1b_2^{-1})^{-1} = b_2b_1^{-1} \in K$. To show $Ka_1b_1 = Ka_2b_2$, it then suffices to show that $(a_1b_1)(a_2b_2)^{-1} \in K$.

Notice that since $b_1b_2^{-1} \in K$, necessarily $a_1b_1b_2^{-1} \in a_1K = Ka_1$ where $a_1K = Ka_1$ since $K \lhd G$. This means there is a $k \in K$ such that

$$a_1b_1b_2^{-1} = ka_1 \qquad \Longrightarrow \qquad a_1b_1b_2^{-1}a_2^{-1} = ka_1a_2^{-1} \in K$$

where $ka_1a_2^{-1} \in K$ since $Ka_1a_2^{-1} = K$. Thus $(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} \in K$, and so the multiplication is well-define, as desired. □

Proposition 35: Let G be a group and K be a subgroup with $K \lhd G$. Let $G/K = \{Ka : a \in G\}$ denote the set of right cosets of K. Then

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

Proof.

1. Notice that by lemma 34 the operation is well-defined, and clearly G/K is closed under the operation. We see that the identity of G/K is $K = K1$. Moreover, since $KaKa^{-1} = Kaa^{-1} = K$, the inverse of Ka is Ka^{-1}. Finally, we see that G/K is associative since G itself is associative, i.e., $Ka(bc) = K(ab)c$ since $a(bc) = (ab)c$ for all $a, b, c \in G$. So G/K is a group, as desired.
2. We see clearly that φ is surjective, since if $Ka \in G/K$, then $\varphi(a) = Ka$. Let $a, b \in G$. Then $\varphi(ab) = Kab = KaKb = \varphi(a)\varphi(b)$, so φ is a homomorphism, as desired.
3. If $[G : K]$ is finite, then by definition $[G : K]$ denotes the set of all distinct right cosets of K, and so $|G/K| = [G : K]$. Also, if G is finite, then by Lagrange's Theorem, $|G/K| = [G : K] = \frac{|G|}{|K|}$, as desired. □

Definition. Quotient Group: Let G be a group and K be a subgroup with $K \lhd G$. The group G/K of all cosets of K in G is called the quotient group of G by K. Moreover, the mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is called the coset map. Recall that the coset map is a surjective homomorphism.

4.2 Isomorphism Theorems

Definition. Group Kernel: Let $\alpha : G \to H$ be a group homomorphism. The kernel of α is defined to be

$$\ker(\alpha) = \{k \in G : \alpha(k) = 1_H\} \subseteq G.$$

Definition. Group Image: Let $\alpha : G \to H$ be a group homomorphism. The image of α is defined to be

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

Lemma 36: Let $\alpha : G \to H$ be a group homomorphism. Then

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

Proof.

1. Note that $1_H = \alpha(1_G) \in \mathrm{im}(\alpha)$ by proposition 20. Let $h_1, h_2 \in \mathrm{im}(\alpha)$ with $h_1 = \alpha(g_1)$ and $h_2 = \alpha(g_2)$, then $h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \mathrm{im}(\alpha)$. Finally, if for $h \in \mathrm{im}(\alpha)$ with $h = \alpha(g)$, we have $h^{-1} = \alpha(g)^{-1} = \alpha(g^{-1}) \in \mathrm{im}(\alpha)$ by proposition 20. Thus by the subgroup test, we see that $\mathrm{im}(\alpha)$ is a subgroup of H.

2. Note that $\alpha(1_G) = 1_H$, so $1_H \in \ker(\alpha)$. Also, note that for $k_1, k_2 \in \ker(\alpha)$ we have

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1_H \cdot 1_H = 1_H$$

and

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1_H^{-1} = 1_H$$

by proposition 20. Thus $k_1^{-1} \in \ker(\alpha)$ and $k_1 k_2 \in \ker(\alpha)$, and so $\ker(\alpha)$ is a subgroup of G by the subgroup test.

Let $k \in \ker(\alpha)$ be arbitrary. Then note for any $g \in G$ we have

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g) \cdot 1_H \cdot \alpha(g)^{-1} = 1_H.$$

Thus we see that $g(\ker(\alpha))g^{-1} \subseteq \ker(\alpha)$, and so $\ker(\alpha) \lhd G$, as desired. □

Example: Consider the determinant map

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \qquad A \mapsto \det(A).$$

Then clearly $\ker(\det) = SL_n(\mathbb{R})$. This provides an alternate proof that $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

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

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

Then $\mathrm{sgn} : S_n \to \{-1, 1\}$ is a homomorphism, and $\ker(\mathrm{sgn}) = A_n$ is the alternating group of degree n (i.e., the set of all even permutations of S_n). This provides another proof that $A_n \lhd S_n$.

Theorem 37. First Group Isomorphism Theorem: Let $\alpha : G \to H$ be a group homomorphism. Then we have $G/\ker(\alpha) \cong \mathrm{im}(\alpha)$.

10/05, lecture 5-2

Proof. Let $K = \ker\alpha$. Since $K \lhd G$, G/K is a group. Define the group map

$$\bar{\alpha} : G/K \to \operatorname{im}\alpha \qquad Kg \mapsto \alpha(g)$$

Note that

$$Kg_1 = Kg_2 \iff g_1 g_2^{-1} \in K \iff \alpha(g_1 g_2^{-1}) = 1 \iff \alpha(g_1) = \alpha(g_2)$$

Thus $\bar{\alpha}$ is well-defined, and an injection. Also $\bar{\alpha}$ is clearly surjective. It remains to show that $\bar{\alpha}$ is a group homomorphism. For $g, h \in G$, we have

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

It follows that $\bar{\alpha}$ is a group homomorphism, and thus a group isomorphism so that $G/K \cong \operatorname{im}\alpha$, as desired. □

Exploration: 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 37. We have then the following diagram

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & H \\ G/K \arrow[ur, "\bar{\alpha}"'] & \end{tikzcd}$$

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

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

Thus $\bar{\alpha}$ is the only homomorphism from G/K to H satisfying $\bar{\alpha}\varphi = \alpha$.

Proposition 38: 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 surjective, and $\bar{\alpha}$ is injective.

Proof. See the above exploration. □

Example: Let $G = \langle g \rangle$ be a cyclic group. Consider the map $\alpha : (\mathbb{Z}, +) \to G$ defined by $\alpha(k) = g^k$ for $k \in \mathbb{Z}$. Clearly α is a surjective (since $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$) group homomorphism. Note that $\ker\alpha = \{k \in \mathbb{Z} : g^k = 1\}$. So we consider two cases:

1. If $o(g) = \infty$, then by proposition 14 $\ker\alpha = \{0\}$. By the first isomorphism theorem, we have $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

2. If $o(g) = n < \infty$, then by proposition 13 $\ker\alpha = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. By the first isomorphism theorem, we have $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

By (1) and (2), we conclude that if G is a cyclic group, then $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$ for some $n \in \mathbb{N}$.

Theorem 39. Second Group Isomorphism Theorem: Let H and K be subgroups of a group G, with $K \lhd G$. Then HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$, and

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

Proof. Since $K \lhd G$, by proposition 30, HK is a subgroup and $HK = KH$ with $K \lhd HK$. Consider the map $\alpha : H \to HK/K$ defined by $\alpha(h) = Kh$. Note that $Kh = K(h1)$ with $h1 \in HK$ with $h \in H$ and $1 \in K$, thus $Kh \in KH/K$. Then we can check that α is a homomorphism (exercise).

Also, if $x \in HK = KH$, say $x = kh$, then $Kx = K(kh) = Kh = \alpha(h)$. So we see that α is surjective. Finally, by proposition 22,

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

since $Kh = K$ if and only if $h \in K$. By the first isomorphism theorem, $HK/K \cong H/(H \cap K)$, as desired. □

Theorem 40. Third Group Isomorphism Theorem: Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then $H/K \lhd G/K$, and

$$^{(G/K)}\big/_{(H/K)} \cong G/H$$

Note that since $K \subseteq H$, if $H \lhd G$, then $K \lhd G$.

Proof. Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Then since $K \subseteq H$, the map is well-defined and is surjective. Note that

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

By the first isomorphism theorem, we have

$$^{(G/K)}\big/_{(H/K)} \cong G/H$$

□

Chapter 5 Group Actions

5.1 Cayley's Theorem

Theorem 41. Cayley's Theorem: If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

10/07, lecture 5-3

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ and let S_G be the permutation group of G. By identifying g_i with $(1 \leq i \leq n)$, we see that $S_G \cong S_n$. Thus to prove this theorem, it suffices to find an injective homomorphism $\sigma : G \to S_G$, as σ is surjective when restricting the co-domain to its image.

For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. Thus 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 $\mu_a \mu_b = \mu_{ab}$ since

$$\mu_a \mu_b(g) = \mu_a(\mu_b(g)) = \mu_a(bg) = abg = \mu_{ab}(g).$$

Also, if $\mu_a = \mu_b$, then $a = \mu_a(1) = \mu_b(1) = b$. Thus σ is an injective homomorphism. By the first isomorphism theorem, we have $G \cong \operatorname{im} \sigma$, which is a subgroup of $S_G \cong S_n$, as desired. □

Remark: Sometimes, we can find a smaller integer m such that G is contained in S_m.

Example: Let H be a subgroup of a group G with $[G : H] = m < \infty$. Let $X = \{g_1 H, g_2 H, \ldots, g_m H\}$ 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 $gH \in X$. Then λ_a is a bijection (exercise) and thus $\lambda_a \in S_x$, the permutation group of X. Consider the map $\tau : G \to S_X$ defined by $\tau(a) = \lambda_a$. For $a, b \in G$ we have $\lambda_{ab} = \lambda_a \lambda_b$ (as in the above proof), and thus τ is a homomorphism. Note that if $a \in \ker \tau$, then $aH = H$, i.e., $a \in H$. Thus $\ker \tau \subseteq H$.

Theorem 42. Extended Cayley's Theorem: Let H be a subgroup of a group G with $[G : H] = m < \infty$. If G has no normal subgroups contained in H, except for $\{1\}$, 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. Then we have $|X| = [G : H] = m$ 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 first isomorphism theorem, we have $G/K \cong \operatorname{im} \tau$. Since $K \subseteq H$ and $K \lhd G$, by the assumption we have that $K = \{1\}$, and so that τ is injective. It follows that $G \cong \operatorname{im} \tau$, a subgroup of $S_X \cong S_m$. □

Corollary 43: 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 $H \lhd G$.

Proof. Let X be the set of all distinct left cosets of H in G. Then we have $|X| = [G : H] = p$ and $S_X \cong S_p$. Let $\tau : G \to S_X \cong S_p$ be the group homomorphism defined in the above example with $K = \ker \tau \subseteq H$. By the first isomorphism theorem, we have $G/K \cong \operatorname{im} \tau \subseteq S_p$. Thus G/K is isomorphic to a subgroup of S_p. Note that $|S_p| = p!$, thus by Lagrange's theorem, we have $|G/K| \mid p!$. Also, since $K \subseteq H$, if $[H : K] = k$, then

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

Thus, since $|G/K| \mid p!$, we have $pk \mid p!$, and so $k \mid (p-1)!$. Since $k \mid |H|$ and $|H| \mid |G|$, and p is the smallest prime dividing $|G|$, we see that every prime divisor of k must be $\geq p$, unless

$k = 1$. However, $k \mid (p-1)!$, thus k has no prime divisors $\geq p$, and so $k = 1$. This implies $K = H$ (because K only has one coset in H, namely K itself, and so $h \in K$ for all $h \in H$, and $K \subseteq H$ from before), and thus $H \lhd G$ since $K \lhd G$. □

5.2 Group Actions

Definition. Group Action: Let G be a group and X a nonempty set. A (left) group action of G on X is a mapping from $G \times X \to X$, 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.

10/17, lecture 6-1

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

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

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

Example: If G is a group, let G act on itself by conjugation, i.e., $a \cdot x = axa^{-1}$ for all $a, x \in G$. Note that $1 \cdot x = 1x1^{-1} = x$. Moreover,

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

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 (see A5) that

1. $\sigma_a \in S_X$, i.e., σ_a is a permutation on X.
2. The function $\theta : G \to S_X$ given by $\theta(a) = \sigma_a$ is a group homomorphism with

$$\ker\theta = \{a \in G : a \cdot x = x \text{ for all } x \in X\}$$

Thus the group homomorphism $\theta : G \to S_X$ gives an equivalent definition of a group action of G on X. If $X = G$ with $|G| = n$ 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. Thus group actions can be viewed as a generalization of the proof of Cayley's Theorem.

Definition. Orbit: Let G be a group acting on a set X, and let $x \in X$. We denote $G \cdot x = \{g \cdot x : g \in G\} \subseteq X$ to be the orbit of x.

Definition. Stabilizer: Let G be a group acting on a set X, and let $x \in X$. We denote $S(x) = \{g \in G : g \cdot x = x\} \subseteq G$ to be the stabilizer of x.

Proposition 44: Let G be a group acting on a set X, and let $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizer 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 $1 \cdot x = x$, we have $1 \in S(x)$. Also, for $g, h \in S(x)$, note that

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

since $g \cdot x = x = h \cdot x$, so $gh \in S(x)$. Finally, note that

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x,$$

and so $g^{-1} \in S(x)$. Thus by the subgroup test, $S(x)$ is a subgroup of G.

2. Write $S(x) = S$. Consider the map $\varphi : G \cdot x \to \{gS : g \in G\}$ define by $\varphi(g \cdot x) = gS$. Note that

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

Thus φ is well-defined and injective. Moreover, φ is clearly surjective, as for any coset gS, we have $\varphi(g \cdot x) = gS$. It follows that $\varphi : G \cdot x \to \{gS : g \in G\}$ is bijective, and so

$$|G \cdot x| = |\{gS : g \in G\}| = [G : S]$$ □

Theorem 45. Orbit Decomposition Theorem: Let G be a group acting on a finite set $X \neq \emptyset$. Let $X_f = \{x \in X : a \cdot x = x \text{ for all } a \in G\}$. Let $G \cdot x_1, G.x_2, \ldots, G \cdot x_n$ denote the distinct non-singleton orbits (i.e., $|G \cdot x_i| > 1$). Then

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

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

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

It follows that the orbits form a disjoint union of X. Since $x \in X_f$ if and only if $G \cdot x = \{x\}$, i.e., $|G \cdot x| = 1$, the set $X \setminus X_f$ contains all non-singleton orbits, which are are disjoint. Thus, by proposition 44

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

10/19, lecture 6-2

Example: Let G be a group acting on itself by conjugation, i.e., $a \cdot x = axa^{-1}$. Then $G_f = \{x \in G : gxg^{-1} = x \ \forall g \in G\}$. We see then that $G_f = Z(G)$ as all elements in G_f commute with all $g \in G$. Also, for $x \in G$ we have

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

This set is called the stabilizer and is denoted by $S(x) = C_G(x)$. That is, $Z(G)$ is the set of elements that commute with all other elements and $C_G(x)$ is the set of elements with which x commutes (then $C_G(x) = G$ if $x \in Z(G)$). Finally, the orbit $G \cdot x = \{gxg^{-1} : g \in G\}$ is called the conjugacy class of x.

Corollary 46. Class Equation: Let G be a finite group and let

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

denote the distinct non-singleton conjugacy classes in G. Then

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

Proof. This follows immediately from the orbit decomposition theorem since the non-singleton conjugacy classes in G are the non-singleton orbits when G acts on itself. Moreover, under this group action $X_f = Z(G)$, as seen in the above example. □

Lemma 47: 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 $X_f = \{x \in X : a \cdot x = x \text{ for all } a \in G\}$. Then we have

$$|X| \equiv |X_f| \pmod p$$

Proof. By the orbit decomposition theorem, we have

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

with $[G : S(x_i)] > 1$ (since $G \cdot x_i$ is non-singleton) for all $1 \le i \le n$. Since $[G : S(x_i)]$ divides $|G| = p^m$ by Lagrange's Theorem and $[G : S(x_i)] > 1$, we have that $p \mid [G : S(x_i)]$ for all $1 \le i \le n$. It follows that $|X| \equiv |X_f| \pmod p$ since the sum $\sum_{i=1}^{n} [G : S(x_i)]$ is a sum of multiples of p. □

Remark: Note that by the above lemma, we see that if $|X| \mid |G|$, then $|X| \equiv 0 \pmod p$. Thus $|X_f| \ge p$ since $1 \in X_f$ and so $|X_f| > 0$, but we also have $|X_f| \equiv |X| \equiv 0 \pmod p$.

Remark: We recall that by Lagrange's Theorem (in particular corollary 24), if a group G is finite and $g \in G$, then $o(g) \mid |G|$. Consider the converse, if $m \mid |G|$, can we find an element $g \in G$ with $o(g) = m$?

Theorem 48. Cauchy's Theorem: Let p be a prime and G be a finite group. If $p \mid |G|$ then G contains an element of order p.

Proof. (J. McKay's Proof) Define

$$X = \{(a_1, a_2, \dots, a_p) : a_i \in G \text{ and } a_1 a_2 \cdots a_p = 1\}.$$

Note that a_p is uniquely determined by $a_1, a_2, \dots, a_{p-1}$ since we must have $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$. Then if $|G| = n$, we have that $|X| = n^{p-1}$ as we can pick any sequence of length $p-1$ of elements in G. Now since $p \mid n$, we have $|X| \equiv 0 \pmod{p}$. Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by "left cycling", i.e., for $k \in \mathbb{Z}_p$,

$$k \cdot (a_1, a_2, \dots, a_p) = (a_{k+1}, a_{k+2}, \dots, a_p, a_1, a_2, \dots, a_k).$$

We can check that this is in fact a well-define group action. Let X_f be defined as in theorem 45. Then $(a_1, a_2, \dots, a_p) \in X_f$ if and only if $a_1 = a_2 = \cdots = a_p$. That is, the only tuples which are fixed under the group action or those where all elements of the tuple are the same.

Clearly $(1, 1, \dots, 1) \in X_f$, and thus $|X_f| \geq 1$. By lemma 47 we have $|X_f| \equiv |X| \equiv 0 \pmod{p}$, thus since $|X_f| \geq 1$, it follows $|X_f| \geq p \geq 2$. Then there is some element $a = (a, a, \dots, a) \in X_f$ with $a \neq 1$. This implies that $a^p = 1$ by definition of X. Since p is a prime, the order of a is p (in particular, by Lagrange's Theorem $o(a) \mid |G|$ but $o(a) \mid p$, thus $o(a) \geq p$). □

Note: This is the end of material covered in test 1.

Chapter 6 Finite Abelian Groups

6.1 Primary Decomposition

Notation: Let G be a group and $m \in \mathbb{Z}$. We define $G^{(m)} = \{g \in G : g^m = 1\}$.

Proposition 49: Let G be an abelian group. Then $G^{(m)}$ is a subgroup of G.

Proof. We have $1 = 1^m \in G^{(m)}$. Since G is abelian we have $(gh)^m = g^m h^m = 1$ for all $g, h \in G^{(m)}$. Also, $(g^{-1})^m = g^{-m} = (g^m)^{-1} = 1^{-1} = 1$. Then by the subgroup test, we see that $G^{(m)}$ is a subgroup of G. □

Proposition 50: Let G be a finite abelian group with $|G| = mk$ with $\gcd(m, k) = 1$. Then

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

10/21, lecture 6-3

Proof. 1. Since G is abelian, we have that $G^{(m)} \lhd G$ and $G^{(k)} \lhd G$ (all subgroups are normal in an abelian group). Since $\gcd(m, k) = 1$, there exists $x, y \in \mathbb{Z}$ such that $mx + ky = 1$. We claim $G^{(m)} \cap G^{(k)} = \{1\}$. To see this, suppose $g \in G^{(m)} \cap G^{(k)}$, then

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

so $g = 1$. Thus we see that $G^{(m)} \cap G^{(k)} = \{1\}$. Further, we claim that $G = G^{(m)}G^{(k)}$. To see this, suppose $g \in G$, then $1 = g^{mk} = (g^k)^m = (g^m)^k$ since $mk = |G|$. It follows then that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Thus

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

Combining our above two claims, we see that by theorem 32 we have that $G = G^{(m)}G^{(k)} \cong G^{(m)} \times G^{(k)}$.

2. Let $|G^{(m)}| = m'$ and $|G^{(k)}| = k'$. We claim that $\gcd(m, k') = 1$. To see this, suppose $\gcd(m, k') \neq 1$, then there exists a prime p such that $p \mid m$ and $p \mid k'$. Then by Cauchy's Theorem, there exists a $g \in G^{(k)}$ with $o(g) = p$ (since $p \mid k' = |G^{(k)}|$). Since $p \mid m$, we also have $g^m = (g^p)^{m/p} = 1$, thus $g \in G^{(m)}$. By (1) we have $g \in G^{(m)} \cap G^{(k)} = \{1\}$. This is a contradiction since $o(g) = p$ and so $g \neq 1$.

   Note that $mk = m'k'$ since $mk = |G| = |G^{(m)} \times G^{(k)}| = m'k'$. Since $m \mid m'k'$ and $\gcd(m, k') = 1$, we have $m \mid m'$. Similarly we get $k \mid k'$. Since $mk = m'k'$, it follows that $m = m'$ and $k = k'$. □

Theorem 51. Primary Decomposition Theorem: Let G be a finite abelian group with $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes and $n_i \in \mathbb{N}$ for all $1 \leq i \leq k$. Then we have

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

Proof. This follows immediately from proposition 50. □

Example: Let $G = \mathbb{Z}_{13}^*$. Then $|G| = 12 = 2^2 \cdot 3$ (since all nonzero elements are invertible). Note that $G^{(4)} = \{a \in \mathbb{Z}_{13}^* : a^4 = 1\} = \{1, 5, 8, 12\}$ and $G^{(3)} = \{a \in \mathbb{Z}_{13}^* : a^3 = 1\} = \{1, 3, 9\}$. Then by theorem 51 we have that $\mathbb{Z}_{13}^* = \{1, 5, 8, 12\} \times \{1, 3, 9\}$.

6.2 p-Groups

Definition. p-Group: Let p be a prime. A p-group is a group in which every element has order equal to a non-negative power of p (including p^0).

Proposition 52: A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. ($\implies$) Consider a proof by contrapositive. Write $|G| = p^n p_2^{n_2}\cdots p_k^{n_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $n, n_2, \ldots, n_k \in \mathbb{N} \cup \{0\}$. If $k \geq 2$, since $p_2 \mid |G|$, by Cauchy's Theorem there exists an element of order p_2, and thus G is not a p-group. By contrapositive it follows that if G is a p-group, then $|G| = p^n$ for some $n \in \mathbb{N} \cup \{0\}$.

($\impliedby$) If $|G| = p^\alpha$ and $g \in G$, then by corollary 24 $o(g) \mid p^\alpha$. Thus $o(g)$ must be a power of p and so G is a p-group. □

Proposition 53: If G is a finite abelian p-group that contains only one subgroup of order p, then G is cyclic. In other words, if a finite abelian group p-group G is not cyclic, then G has at least two subgroups of order p.

Proof. Let $y \in G$ be an element of maximal order, i.e., $o(y) \geq o(x)$ for all $x \in G$. We claim that $G = \langle y \rangle$. To see this, suppose that $G \neq \langle y \rangle$. Then the quotient group $G/\langle y \rangle$ is a non-trivial p-group (since it'll have order of a power of p). Then by Cauchy's Theorem, there exists a $z \in G/\langle y \rangle$ of order p. In particular, $z \neq 1$. Consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ with $\pi(x) = z$. Since $\pi(x^p) = \pi(x)^p = z^p = 1_{G/\langle y \rangle}$ (since the coset map is a homomorphism) or equivalently $x^p\langle y \rangle = \langle y \rangle$, we see that $x^p \in \langle y \rangle$. Thus $x^p = y^m$ for some $m \in \mathbb{Z}$. We consider two cases:

Case 1. If $p \nmid m$, since $o(y) = p^r$ for some $r \in \mathbb{N}$ (G is a p-group), then by proposition 18, $o(y^m) = o(y)$. Since y is of maximal order, we have

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

which is a contradiction. Note we get $o(x^p) < o(x)$ since $p \mid o(x)$ (since $x \neq 1$ and G is a p-group) and so by proposition 15 $o(x^p) = \frac{o(x)}{p} < o(x)$. Note that $x \neq 1$ since $\pi(x) = z$ and $z \neq 1$, however, $\pi(1) = 1$ by proposition 20.

Case 2. If $p \mid m$, then $m = pk$ for some $k \in \mathbb{Z}$. Thus $x^p = y^m =^{pk}$. Since G is abelian we have $(xy^{-k})^p = x^p y^{-pk} = y^m y^{-m} = 1$. Thus xy^{-k} belongs to the only one subgroup of order p, say H. Since $\langle y \rangle$ contains a subgroup of order p, we have $H \subseteq \langle y \rangle$. Thus $xy^{-k} \in \langle y \rangle$, which implies $x \in \langle y \rangle$. If follows that $z = \pi(x) = 1$ since $x \in \langle y \rangle$, a contradiction since $o(z) = p$.

By combining the above two cases, we see that $G = \langle y \rangle$. □

10/24, lecture 7-1

Proposition 54: Let $G \neq \{1\}$ be a finite abelian p-group. Let C be a cyclic subgroup of maximal order. Then G contains a subgroup B such that $G = CB$ and $C \cap B = \{1\}$. Then by Theorem 32, we have that $G \cong C \times B$.

Proof. Suppose $G \neq C$, then G has two cyclic groups of order p by proposition 53. Then there exists a cyclic group $D \not\subseteq C$ with $|D| = p$. Then we will show by induction that $\pi : G \to G/D$

We prove this result by induction. If $|G| = p$, we take $C = G$ and $B = \{1\}$. Suppose the result holds for all groups of order p^{n-1} with $n \in \mathbb{N}$ and $n \geq 2$. We will prove that the result holds for $|G| = p^n$. We consider two cases

Case 1. If $C = G$, then by taking $B = \{1\}$ the result holds.

Case 2. If $C \neq G$, then we know that G is not cyclic (since C is maximal). By proposition 53, there exists at least two subgroups of order p. Since C is cyclic, by theorem 19, 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 $C \cap D = \{1\}$ since $C \cap D$ is a subgroup of D and by Lagrange's theorem D only has subgroups of order p or 1 (if $|C \cap D| = p$ then $C \cap D = D$ and so $D \subseteq C$, a contradiction).

Consider the coset map $\pi : G \to G/D$. If we consider $\pi|_C$, the restriction of π on C, then $\ker(\pi|_C) = C \cap D = \{1\}$. Thus by the first isomorphism theorem, $\pi(C) \cong C$. Let y be a generator of the cyclic group C, i.e., $C = \langle y \rangle$. Since $\pi(C) \cong C$ we have $\pi(C) = \langle \pi(y) \rangle$. By the assumption on C, $\pi(C)$ is a cyclic subgroup of G/D of maximal order. Since $|G/D| = p^{n-1}$, by the induction hypothesis, G/D has a subgroup E such that $G/D = \pi(C)E$ and $\pi(C) \cap E = \{1\}$.

Let $B = \pi^{-1}(E)$, i.e., B is the preimage, or equivalently the subgroup of maximal order such that $\pi(B) = E$ since π is surjective but not necessarily invertible. We claim that $G = CB$. To see this, note that since E is a subgroup containing $\{1\}$, we have $\pi^{-1}(\{1\}) = D \subseteq B$. If $x \in G$, since $\pi(C)\pi(B) = \pi(C)E = G/D$, there exists a $u \in C$ and $v \in B$ such that $\pi(x) = \pi(u)\pi(v)$. Then since π is a homomorphism and G is abelian, $\pi(xu^{-1}v^{-1}) = \pi(1) = 1 \in E$, and thus $xu^{-1}v^{-1} \in B$. Note we then also have $xu^{-1}v^{-1}v = xu^{-1} \in B$ since $v \in B$. Since G is abelian, we have $x = uxu^{-1} \in CB$. Thus the claim holds.

We also claim that $C \cap B = \{1\}$. Let $x \in C \cap B$. Then $\pi(x) \in \pi(C) \cap \pi(B) = \{1\}$. Since $\pi(x) = 1_{C/D}$, we have $x \in D$. Since $x \in C \cap D = \{1\}$ as a result, we see that $x = 1$. Combining our above two claims, the result follows. $\square$

Theorem 55: Let $G \neq \{1\}$ be a finite abelian p-group. Then G is isomorphic to a direct product of cyclic groups.

Proof. By proposition 54, there exists a cyclic group C_1 and a subgroup B_1 of G such that $G \cong C_1 \times B_1$. Since $|B_1| \mid |G|$, the group B_1 is also a p-group. Thus if $B_1 \neq \{1\}$, by proposition 54, there exists a cyclic group C_2 and a subgroup B_2 such that $B_1 \cong C_2 \times B_2$. We repeat this process until we get cyclic groups $C_1, \ldots, C_k$ and $B_k = \{1\}$. Then $G \cong C_1 \times \cdots \cong C_k$. $\square$

10/26, lecture 7-2

Remark: One can show that if G is a finite abelian p-group and

$$G \cong C_1 \times C_2 \times \cdots C_k \cong D_1 \times \cdots \times D_\ell$$

are two decompositions of G as a product of cyclic groups C_i and D_j of order p^{n_i} and p^{m_j} respectively. Then $k = \ell$ and after some reordering $n_1 = m_1, \ldots, n_k = m_k$

Theorem 56. Fundamental/Structure Theorem of Finite Abelian Groups: If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

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 $1 \leq i \leq k$). The numbers $p_i^{n_i}$ are uniquely determined up to their order. Note that if p_1 and p_2 are distinct primes, then $C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}}$.

Theorem 57. Invariant Factor Decomposition of Finite Abelian Groups: Let G be a finite abelian group. Then

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \mathbb{Z}_{n_r}$$

where $n_i \in \mathbb{N}$, $n_1 \geq 1$, and $n_1 \mid n_2 \mid n_3 \mid \cdots \mid n_r$.

Example: Let G be an abelian group of order 48. Since $48 = 2^4 \cdot 3$, by theorem 51, $G \cong H \times \mathbb{Z}_3$ where H is abelian group of order 2^4. The options for H are

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

Thus the options for G are

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

Chapter 7 Rings

7.1 Rings

Definition. Ring: A set R is a ring if it has two operations, addition $+$ and multiplication $\cdot$ such that $(R, +)$ is an abelian group and $(R, \cdot)$ satisfies closure, associativity, and identity properties of a group, in addition to a distributive law. Note that $(R, \cdot)$ does not necessarily have an inverse for all elements. Then more precisely R is a ring if and only if for all $a, b, c \in R$ we have

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 $0 + a = a = a + 0$ (0 is called the zero of R)
5. For $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$.
6. $ab = a \cdot b \in R$
7. $a(bc) = (ab)c$

8. There exists $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ (1 is called the unity of R)
9. $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ (distributive laws)

The ring R is said to be a commutative ring if it also satisfies

10. $ab = ba$

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

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

Example: For $n \in \mathbb{N}$ with $n \geq 2$, the set $\mathsf{M}_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication. The zero is the zero matrix O and the unity being the identity matrix I. Note that since matrix multiplication is not necessarily commutative, $\mathsf{M}_n(\mathbb{R})$ is not a commutative ring.

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

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

$$na = \underbrace{a + a + a + \cdots + a}_{n \text{ times}}$$

and

$$a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}.$$

One can show that $0 \cdot a = 0$ (see proposition 57) and we define $a^0 = 1$. Also, we define

$$(-n) \cdot a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}} = n(-a).$$

If the multiplicative inverse of a exists, say a^{-1}, then we define

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ times}} = (a^{-1})^n$$

note that the above is thus not necessarily defined. We recall that for a group G and $g \in G$, we have $g^0 = 1$, $g^1 = g$, and $(g^{-1})^{-1} = g$. Thus for addition we have

$$0 \cdot a = 0_R, \qquad 1 \cdot a = a, \qquad -(-a) = a$$

where the first 0 is from $\mathbb{Z}$ but the second 0_R is the zero of our ring. Also by proposition 2, for $n, m \in \mathbb{Z}$

$$(na) + (ma) = (n+m)a, \qquad n(ma) = (nm)a, \qquad n(a+b) = na + nb.$$

We can also prove the following proposition (see Piazza).

Proposition 58: Let R be a ring and $r, s \in R$. Then

1. If 0 is the zero of R, then $0 \cdot r = 0 = r \cdot 0$ (all 0's here are from R, not $\mathbb{Z}$).
2. $(-r)s = -(rs) = r(-s)$
3. $(-r)(-s) = rs$
4. For any $m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$.

Proof.

1. Notice $r^2 + 0 = r^2 = r(r + 0) = r^2 + r0$, thus since $(R, +)$ is a group, by cancellation we have $0 = r0$. Similarly we can find $0r = 0$.
2. Notice $rs + (-r)s = (r - r)s = 0s = 0$ by (1), thus $(-r)s = -(rs)$. Similarly we can find $r(-s) = -(rs)$.
3. Notice $(-r)(-s) = -(r(-s)) = -(-(rs))$. Since $rs+(-rs) = 0$, we see $-(-(rs)) = rs$.
4. Can prove by induction on m. □

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

Remark: If R is a ring with $R \neq \{0\}$ (i.e., R is not a trivial ring), since $r = r \cdot 1$ for all $r \in R$ and $0 = r \cdot 0$, we have $1 \neq 0$.

Example. Ring Direct Product: Let $R_1, R_2, \ldots, R_n$ be rings. We define componentwise operations on the product $R_1 \times R_2 \times \cdots \times R_n$ as follows:

$$(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)$$

and

$$(r_1, r_2, \ldots, r_n) \cdot (s_1, s_2, \ldots, s_n) = (r_1 s_1, r_2 s_2, \ldots, r_n s_n)$$

One can check that $R_1 \times \cdots \times R_n$ is a ring with the zero being the n-tuple $(0, 0, \ldots, 0)$ and the unity being the n-tuple $(1, 1, \ldots, 1)$. This set $R_1 \times \cdots \times R_n$ is called the direct product of $R_1, R_2, \ldots, R_n$.

10/31, lecture 8-1

Definition. Characteristic of Rings: If R is a ring, we define the characteristic of R, denote $\mathrm{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$. In particular,

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

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean $kr = 0$ for all $r \in R$. By Prop 58, we have $kr = k(1_R \cdot r) = (k \cdot 1_R)r$. Thus $kR = 0$ if and only if $k1_R = 0$ by proposition 13 and 14.

Proposition 59: Let R be a ring and $k \in \mathbb{Z}$. Then

1. If $\mathrm{ch}(R) = n \in \mathbb{N}$, then $kR = 0$ if and only if $n \mid k$.

2. If $\text{ch}(R) = 0$, then $kR = 0$ if and only if $k = 0$.

Proof. 1. Recall $kR = 0$ if and only if $k1_R = 0$, by proposition 13, this is true if and only if $n \mid k$.

2. Recall $kR = 0$ if and only if $k1_R = 0$, by proposition 14, this is true if and only if $k = 0$. □

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

7.2 Subrings

Definition. Subring: A subset S of a ring R is a subring if S is a ring itself with $1_S = 1_R$. Generally we assume S has the same addition and multiplications operations as R.

Note. Subring Test: Note that properties (2), (3), (7), (9) of a ring are automatically satisfied. Thus to show S is a subring, it sufficient to check the following:

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 $-t = 0 - t \in S$ and S is closed under addition

Example: Note that it is not necessarily the case that $1_S = 1_R$ if $S \subseteq R$ is a ring R. For instance, take $R = \mathbb{Z}_{30}$ and $S = \{[0], [6], [12], [18], [24]\}$. Then $1_R = [1]$ and $1_S = [6]$, for instance. Another example is to take $R = \mathsf{M}_2(\mathbb{R})$ and

$$S = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R} \right\}$$

Thus

$$1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad 1_S = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Remark: Sometimes, it is convenient to allow $1_S \neq 1_R$. For example, if $R = \mathbb{Z}_{30}$ and $S = \{[0], [6], [12], [18], [24]\}$, then $1_R = [1]$ and $1_S = [6]$. However, in this class, we'll only take $1_S = 1_R$.

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

Example. Center of Ring: If R is a ring, the center $Z(R)$ of R is defined to be

$$Z(R) = \{z \in R : zr = rz \quad \text{for all } r \in R\}$$

Note that $1 \in Z(R)$. Also, for any $s, t \in Z(R)$, then for all $r \in R$,

$$(s-t)r = sr - tr = rs - rt = r(s-t) \qquad \text{and} \qquad (st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st).$$

So by the subring test, we see that $Z(R)$ is a subring of R.

Example. Gaussian Integers: Let $Z[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\} \subseteq \mathbb{C}$. Then one can show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, called the ring of Gaussian Integers.

7.3 Ideals

Note: Let R be a ring and let A an additive subgroup of R. Since $(R, +)$ is abelian, we have that $A \triangleleft R$. Thus, we have the additive quotient group $R/A = \{r + A : r \in R\}$ with $r + A = \{r + a : a \in A\}$. Using the known properties of cosets and quotient groups, we have the following proposition.

Proposition 60: Let R be a ring and let A be an additive subgroup of R. For $r, s \in R$, we have

1. $r + A = s + A$ if and only if $(r - s) \in A$.
2. $(r + A) + (s + A) = (r + s) + A$.
3. $0 + A = A$ is the (additive) identity of R/A.
4. $-(r + A) = (-r) + A$ is the (additive) inverse of $r + A$.
5. $k(r + A) = (kr) + A$ for all $k \in \mathbb{Z}$. (Recall this isn't the ring's multiplication but rather the k time sum of $(r + A)$.)

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

$$(r + A)(s + A) = rs + A \tag{*}$$

Note that we could have $r_1 + A = r_2 + A$ and $s_1 + A = s_2 + A$ with $r_1 \neq r_2$ and $s_1 \neq s_2$. Thus in order for (*) to make sense, a necessary condition is

$$r_1 + A = r_2 + A \quad \text{and} \quad s_1 + A = s_2 + A \quad \implies \quad r_1 s_1 + A = r_2 s_2 + A$$

In this case, we say the multiplication $(r + A)(s + A)$ is well-defined.

Proposition 61: Let A be an additive subgroup of a ring R. For $a \in A$, define $Ra = \{ra : r \in R\}$ and $aR = \{ar : r \in R\}$. Then the following are equivalent

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

Proof. ($1 \implies 2$) If $r_1 + A = r_2 + A$ and $s_1 + A = s_2 + A$, we need to show $r_1 s_1 + A = r_2 s_2 = A$, i.e., $r_1 s_1 - r_2 s_2 \in A$. Since $(r_1 - r_2) \in A$ and $(s_1 - s_2) \in A$, we have

$$\begin{aligned} r_1 s_1 - r_2 s_2 &= r_1 s_1 - r_2 s_1 + r_2 s_1 - r_2 s_2 \\ &= (r_1 - r_2) s_1 + r_2 (s_1 - s_2) \\ &\in (r_1 - r_2) R + R(s_1 - s_2) \subseteq A \qquad \text{by (1)} \end{aligned}$$

Thus we see $r_1s_1 - r_2s_2 \in A$ so that $r_1s_1 + A = r_2s_2 + A$.

($2 \implies 1$) Let $r \in R$ and $a \in A$. By proposition 58, we have

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = r \cdot 0 + A = 0 + A = A$$

Thus $ra \in A$ and we have $Ra \subseteq A$. By a similar argument, $aR \subseteq A$. □

Definition. Ideal: An additive subgroup A of a 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 $ra \in A$.

11/02, lecture 8-2

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

Proposition 62: Let A be an ideal of a ring R. If $1_R \in A$ then $A = R$.

Proof. For every $r \in R$, since A is an ideal and $1_R \in A$, we have $r = r1_R \in A$ □

Proposition 63: Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with multiplication $(r + A)(s + A) = rs + A$. The unity of R/A is $1 + A$.

Proof. Follows by proposition 61. □

Definition. Quotient Ring: Let A be an ideal of a ring R. The ring R/A is called the quotient ring of R by A.

Definition. Generated Principal Ideals: Let R be a commutative ring and A an ideal of R. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in R$, we say A is the principal ideal generated by a and is denoted 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 64: 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 is generated by 0. Otherwise, choose $a \in A$ with $a \neq 0$ such that $|a|$ is minimal. Clearly, $\langle a \rangle \subseteq A$. To prove the other inclusion, let $b \in A$. By the division algorithm, we have $b = qa + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$. If $r \neq 0$, since A is an ideal and $a, b \in A$, we have $r = b - qa \in A$ with $|r| < |a|$, a contradiction by the minimality of a. Thus $r = 0$ and $b = qa$, i.e., $b \in \langle a \rangle$. We see then that $A = \langle a \rangle$. □

7.4 Isomorphism Theorems

Definition. 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. $\theta(1_R) = 1_S$

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

Example: If R_1 and R_2 are rings, the projections $\pi_1 : R_1 \times R_2 \to R_1$, defined by $\pi_1(r_1, r_2) = r_1$ is a surjective ring homomorphism. So is $\pi_2 : R_1 \times R_2 \to R_2$ with $\pi_2(r_1, r_2) = r_2$.

Proposition 65: Let $\theta : R \to S$ be a ring homomorphism and let $r \in R$. Then

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

Proof.

1. Notice $\theta(0_R) = \theta(0_R + 0_R) = \theta(0_R) + \theta(0_R)$, thus by cancellation (under $(S, +)$) we have $\theta(0_R) = 0_S$.
2. Notice for any $r \in R$ we have $\theta(r) + \theta(-r) = \theta(r - r) = \theta(0_R) = 0_S$ by (1), thus $\theta(-r) = -\theta(r)$.
3. Provable by induction on k.
4. Provable by induction on n.
5. By (4), it suffices to show $\theta(u^{-1}) = \theta(u)^{-1}$. To see this note $\theta(u)\theta(u^{-1}) = \theta(uu^{-1}) = \theta(1_R) = 1_S$, thus $\theta(u^{-1}) = \theta(u)^{-1}$. □

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

Definition. Ring Kernel: Let R and S be rings. If $\theta : R \to S$ is a ring homomorphism, the kernel of θ is defined by

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

Definition. Ring Image: Let R and S be rings. If $\theta : R \to S$ is a ring homomorphism, the image of θ is defined by

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

Proposition 66: Let $\theta : R \to S$ be a ring homomorphism. Then

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

Proof.

1. Let $y_1, y_2 \in \operatorname{im}\theta$ and $x_1, x_2 \in R$ such that $\theta(x_1) = y_1$ and $\theta(x_2) = y_2$. Then notice $y_1 - y_2 = \theta(r_1) - \theta(r_2) = \theta(r_1 - r_2) \in \operatorname{im}\theta$ and $y_1y_2 = \theta(r_1)\theta(r_2) = \theta(r_1r_2) \in \operatorname{im}\theta$. Thus by the subring test $\operatorname{im}\theta$ is a subring of S.
2. Let $x, y \in \ker\theta$. Then notice $\theta(x - y) = \theta(x) - \theta(y) = 0_S - 0_S = 0_S$ and $\theta(xy) = \theta(x)\theta(y) = 0_S0_S = 0_S$. Thus by the subring test $\ker\theta$ is a subring of R. Let $r \in R$. Then notice that $\theta(xr) = \theta(x)\theta(r) = 0_S\theta(r) = 0_S$ so $xr \in \ker\theta$. Similarly we can show $rx \in \ker\theta$ so that $\ker\theta$ is an ideal of R. □

Proposition 67. First Ring 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, 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 if

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

Thus $\bar{\theta}$ is injective and well-defined. Also clearly $\bar{\theta}$ is clearly surjective. One can also check that $\bar{\theta}$ is a ring homomorphism. Thus $\bar{\theta}$ is a ring isomorphism, and thus $R/\ker\theta \cong \operatorname{im}\theta$. □

Theorem 68. Second Ring Isomorphism Theorem: Let A be a subring and B be an ideal of a ring 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

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

Proof. See A7. □

Theorem 69. Third Ring Isomorphism Theorem: Let A and B be ideals of a ring R with $A \subseteq B$. Then B/A is an ideal in R/A and

$$^{(R/A)}\big/_{(B/A)} \cong R/B$$

Proof. See A7. □

11/04, lecture 8-3

Theorem 70. Chinese Remainder Theorem: Let R be a ring and A, B be ideals of R. Then

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). Thus it suffices to prove (1). Define

$$\theta : R \to R/A \times R/B \qquad \theta(r) = (r + A, r + B)$$

for all $r \in R$. Then θ is a ring homomorphism (exercise). To show θ is surjective, let $(s + A, t + B) \in R/A \times R/B$ with $s, t \in R$. Since $A + B = R$, then there exists $a \in A$ and $b \in B$ such that $a + b = 1$. Let $r = sb + ta$. Then

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

Note $(s - t)a \in A$ since A is an ideal. Thus $s + A = r + A$. Similarly $t + B = r + B$. Thus $\theta(r) = (r + A, r + B) = (s + A, t + B)$. Thus $\operatorname{im}\theta = R/A \times R/B$. Since $\ker\theta = A \cap B$, by the first isomorphism theorem, we have

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

□

Example: Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. We have $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ and $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. By the Chinese Remainder Theorem, we have the following corollary.

Corollary 71:

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 $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$ where $\varphi(m) = |\mathbb{Z}_m^*|$ is the Euler Totient (Phi) Function.

Remark: By corollary 71, if $x \equiv a \pmod{m}$ and $x \cong b \pmod{n}$, there exists a unique solution of these simultaneous congruence of the form $x \cong c \pmod{mn}$. Notice is this is the standard statement of the Chinese Remainder Theorem in MATH 135.

Proposition 72: If R is a ring with $|R| = p$, for a prime p. Then $R \cong \mathbb{Z}_p$.

Proof. Define $\theta : \mathbb{Z}_p \to R$ by $\theta([k]) = k1_R$. Note that since R is also an additive group and $|R| = p$, by Lagrange's Theorem, $o(1_R) = 1$ or $o(1_R) = p$. Since $1_R \neq 0$ (since $p \geq 2$), we have $o(1_R) = p$. Thus

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

Thus θ is well-defined and injective. Also θ is a ring homomorphism (exercise). Since $|\mathbb{Z}_p| = p = |R|$ and θ is injective, we have that θ is surjective. It follows that θ is a ring isomorphism and thus $R \cong \mathbb{Z}_p$. □

Chapter 8 Commutative Rings

8.1 Integral Domains and Fields

Definition. Unit: Let R be a ring. We say $u \in R$ is a unit if u has a multiplicative inverse in R, denoted by $u^{-1} \in R$. We have that $uu^{-1} = 1 = u^{-1}u$. Note that if u is a unit in R and $r, s \in R$, then

$$ur = us \implies r = s \qquad \text{and} \qquad ru = su \implies r = s$$

Let R^* denote the set of all units in R. One can show that $(R^*, \cdot)$ is a group, called the group of unity of R.

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

Example: Consider $\mathbb{Z}[i]$. Then $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Definition. Division Ring: A ring $R \neq \{0\}$ is a division ring if $R^* = R \setminus \{0\}$. A commutative division ring is a field.

Example: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

Example: We recall that $[a][x] = [1]$ in $\mathbb{Z}_n$ has a solution if and only if $\gcd(a, n) = 1$. Thus if $n = p$ is prime, then $\gcd(a, p) = 1$ for all $a \in \{[1], [2], \ldots, [p-1]\}$. Thus $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ and so $\mathbb{Z}_p$ is a field. However, if n is not a prime, say $n = ab$ with $a, b < n$, then $[a]$ has no inverse. Hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n \setminus \{0\}$ if n is not prime. Thus $\mathbb{Z}_n$ is a field if and only if n is a prime.

Remark: If R is a division ring (or a field), then R's only ideals are $\{0\}$ and R, since if $A \neq \{0\}$ is an ideal, then $0 \neq a \in A$ implies that $1 = a \cdot a^{-1} \in A$. By proposition 62, $A = R$.

Note: There is a theorem, Wedderburn's Little Theorem, which shows that every finite division ring is a field.

Example: Let $n \in \mathbb{N}$ with $n = ab$ with $1 < a, b < n$. Then $[a][b] = [n] = [0]$, but $[a] \neq [0]$ and $[b] \neq [0]$.

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

Example: Note that $[2], [3], [4]$ are zero divisor of $\mathbb{Z}_6$.

Example: The matrix

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

is a zero divisor of $\mathsf{M}_2(\mathbb{R})$ since

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

11/07, lecture 9-1

Proposition 73: Given a ring 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. Note the above is saying that these implications are equivalent, e.g., if a is not a zero-divisor then it satisfies cancellation laws. We prove ($1 \iff 2$), the proof of ($1 \iff 3$) is similar.

($1 \implies 2$) Let $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$, by (1), since $a \neq 0$, we have $b - c = 0$, i.e., $b = c$.

($2 \implies 1$) Let $ab = 0$ in R. We consider two cases. If $a = 0$ then we are done. Otherwise, suppose $a \neq 0$, then we have $ab = 0 = a0$, then by (2) we have $b = 0$. □

Definition. 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 $b = 0$, and so by the above proposition we have cancellation.

Example: $\mathbb{Z}$ is an integral domain since $ab = 0$ implies $a = 0$ or $b = 0$.

Example: $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

Proposition 74: Every field is an integral domain.

Proof. Let $ab = 0$ in a field R. We consider two cases. If $a = 0$ we are done. Otherwise, suppose $a \neq 0$. Then since $a \neq 0$ and R is a field, $a \in R^*$ and so $a^{-1} \in R$ exists. Then

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

Thus R is an integral domain by proposition 73. □

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

Note: The converse of proposition 74 is not necessarily true. For instance, $\mathbb{Z}$ is an integral domain, but not a field.

Proposition 75: Every finite integral domain is a field.

Proof. Let R be a finite integral domain, say $|R| = n$. Write $R = \{r_1, r_2, \ldots, r_n\}$. Given $a \neq 0$ in R, by proposition 73, we have that the set $aR = \{ar_1, ar_2, \ldots, ar_n\}$ has distinct elements since if $ar_i = ar_j$, then by proposition 73 $r_i = r_j$. Since $|aR| = n$ and $aR \subseteq R$. In particular, $1 \in aR$, say $1 = ab$ for some $b \in R$. Since R is commutative, we have $ab = 1 = ba$, i.e., a is a unit. Thus R is a field. □

Remark: We recall the characteristic of a ring R, denoted $\text{ch}(R)$, is the order of 1_R in $(R,+)$. In particular

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

Proposition 76: The characteristic of an integral domain is either 0 or a prime p.

Proof. Let R be an integral domain. We consider two cases. If $\text{ch}(R) = 0$, then we are done. Otherwise suppose $\text{ch}(R) = n \in \mathbb{N}$. Suppose that n is not a prime, say $n = ab$ with $1 < a, b < n$. If 1 is the unity of R, then by proposition 58 we have $(a \cdot 1)(b \cdot 1) = (ab)(1 \cdot 1) = n \cdot 1 = 0$. Then since R is an integral domain, either $a \cdot 1 = 0$ or $b \cdot 1 = 0$ and thus $o(1) = a$ or $o(1) = b$ respectively. This is a contradiction since $o(1) = n$ and $n \neq a$ and $n \neq b$. Thus n must be prime. □

Remark: Let R be an integral domain with $\text{ch}(R) = p$ for a prime p. For $a, b \in R$, we have by the binomial theorem that

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

Note that for any $0 < r < p$ we have

$$\binom{p}{r} = \frac{p!}{(p-r)!r!},$$

however, since $r > 0$ we have $p - r < p$ and so the above is a multiple of p. Thus since $p \cdot r = (p \cdot 1)r = 0 \cdot r = 0$ for all $r \in R$, we then have $(a+b)^p = a^p + b^p$.

8.2 Prime Ideals and Maximal Ideals

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

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

Example: For $n \in \mathbb{N}$ with $n \geq 2$, we have that $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proposition 77: If R is a commutative ring, then an ideal P of R is a prime ideal if and only if 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 if and only if $rs \in P$ implies that $r \in P$ or $s \in P$. However, this is true if and only if $(r+P)(s+P) = 0 + P$ implies that $r + P = 0 + P$ or $s + P = 0 + P$, which is equivalent to saying that R/P is an integral domain. □

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

Proposition 78: If R be a commutative ring, then an ideal M of R is maximal if and only if R/M is a field.

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

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

Also, for $r \in R$, note that $r \notin M$ if and only if $r + M \neq 0 + M$. Thus we have that that M is a maximal ideal if and only if $\langle r \rangle + M = R$ for any $r \notin M$ (since $M \subseteq \langle r \rangle + M$ is ideal and M is maximal), if and only if $1 \in \langle r \rangle + M$, if and only if for any $r + M \neq 0 + M$, there exists an $s + M \in R/M$ such that $(r + M)(s + M) = 1 + M$, if and only if R/M is a field. □

11/09, lecture 9-2

Corollary 79: Every maximal ideal of a commutative ring is a prime ideal.

Proof. By combining propositions 74, 77, and 78. □

Remark: The converse of corollary 79 is not necessarily true. For instance, in $\mathbb{Z}$, $\{0\}$ is a prime ideal but not a maximal ideal.

8.3 Fields of Fractions

Remark: We recall that every subring of a field is an integral domain. We might ask if an integral domain is a subring of a field?

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

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

We say $(r_1, s_1) \equiv (r_2, s_2)$ on X if and only if $r_1 s_2 = s_1 r_2$. We can show that $\equiv$ defines an equivalence relation on X (exercise). More precisely, we have the following for any $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in X$:

1. $(r_1, s_1) \equiv (r_1, s_1)$
2. $(r_1, s_1) \equiv (r_2, s_2) \iff (r_2, s_2) \equiv (r_1, s_1)$
3. If $(r_1, s_1) \equiv (r_2, s_2)$ and $(r_2, s_2) \equiv (r_3, s_3)$, then $(r_1, s_1) \equiv (r_3, s_3)$.

Motivated by the case $R = \mathbb{Z}$, we now define fraction $\frac{r}{s}$ to be the equivalence class $[(r, s)]$ on X. Note the equivalence class is

$$\frac{r}{s} = [(r, s)] = \{(r', s') \in X : (r, s) \equiv (r', s')\} = \{(r', s') \in X : rs' = r's\}.$$

Let F denote the set of all these fractions. I.e.,

$$F = \{\tfrac{r}{s} : r \in R \text{ and } s \in D\} = \{\tfrac{r}{s} : r \in R \text{ and } s \in R \setminus \{0\}\}$$

The addition and multiplication operations on F are defined by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2} \qquad \text{and} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Note that $s_1 s_2 \neq 0$ since R is an integral domain. Hence these operations are well-defined. We can show that F is a field with the zero being $\frac{0}{1}$, the unity being $\frac{1}{1}$, and the negative of $\frac{r}{s}$ being $\frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0$ in F, then $r \neq 0$ and $\frac{s}{r} \in R$ with $\frac{r}{s} \cdot \frac{s}{r} = \frac{1}{1}$. Also, we have $R \cong R'$ where $R' = \{\frac{r}{1} : r \in R\} \subseteq F$. We thus get the following theorem.

Theorem 80: 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 (R is isomorphic to a subring of F). The field F is called the field of fractions of R.

Proof. See the above exploration. □

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

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

Then we can show that the corresponding set of fractions F is an integral domain, which contains R. Such and F is called the ring of fractions of R over D and it is donated by $D^{-1}R$. Note that F is an integral domain, though not necessarily a field.

Remark: If R is an integral domain and P is a prime ideal of R, then $D = R \setminus P$ satisfies the conditions we specified above. The resulting ring $D^{-1}R$ is called a localization of R at the prime ideal P.

Chapter 9 Polynomial Rings

9.1 Polynomial Rings

Exploration: Let R be a ring. Let x be a variable (i.e., an indeterminate) Let

$$R[x] = \{f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : n \in \mathbb{N} \cup \{0\}, a_i \in R\}.$$

Such an $f(x) \in R[x]$ is called a polynomial in x over R. If $a_m \neq 0$, we say that $f(x)$ has degree m, denoted $\deg f = m$, and we say a_m is the leading coefficient of $f(x)$. If $\deg f = 0$, then $f(x) = a_0 \in R$, in this case we say $f(x)$ is a constant polynomial. Note that if

$$f(x) = 0 \quad \iff \quad a_0 = a_1 = a_2 = \cdots = a_m = 0,$$

we define $\deg 0 = -\infty$ (we'll see why later). Let

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x] \qquad \text{and} \qquad g(x) = b_0 + b_1 x + \cdots + b_n x^n \in R[x]$$

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

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots (a_n + b_n)x^n \\ f(x)g(x) &= (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots \\ &= c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n} \end{aligned}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$.

Proposition 81: Let R be a ring and let x be a variable. Then

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

Proof. (1) and (2) are left as exercises. Let

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in Z[x] \qquad \text{and} \qquad g(x) = b_0 + b_1 + \cdots + b_n x^n \in R[x].$$

Then

$$f(x)g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n} \qquad \text{where} \qquad c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0.$$

Since $a_i \in Z(R)$, we have $a_i b_j = b_j a_i$ for all i, j. Thus $f(x)g(x) = g(x)f(x)$, and so $Z[x] \subseteq Z(R[x])$.

To show the other inclusion, note that if $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in Z(R[x])$, then $f(x)b = bf(x)$ for all $b \in R$. It follows that $a_i b = b a_i$ for all $0 \leq i \leq m$. It implies that $a_i \in Z$ and hence we have $Z(R[x]) \subseteq Z[x]$. Thus $Z(R[x]) = Z[x]$. □

11/11, lecture 9-3

Note: **Warning:** Although $f(x) \in R[x]$ can be used to defined 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 82: 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. ((1) and (2)) Suppose $f(x) \neq 0$ and $g(x) \neq 0$. Say

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \qquad \text{and} \qquad g(x) = b_0 + b_1 + \cdots + b_n x^n$$

with $a_m \neq 0$ and $b_n \neq 0$. Then $f(x)g(x) = (a_m b_n)a^{m+n} + \cdots + a_0 b_0$. Since R is an integral domain, $a_m b_n \neq 0$ and thus $f(x)g(x) \neq 0$. It follows that $R[x]$ is an integral domain. Moreover, $\deg(fg) = \deg(f) + \deg(g)$.

(3) Suppose that $u(x)$ is a unit in $R[x]$, say $u(x)v(x) = 1$. By (2),

$$\deg(u) + \deg(v) = \deg(1) = 0,$$

and so $\deg(u) = 0 = \deg(v)$. Thus $u(x)$ and $v(x)$ are units in R. □

Remark: In $\mathbb{Z}_4$, we have $(2x)(2x) = 4x^2 = 0$, thus $\deg(2x) + \deg(2x) \neq \deg(2x \cdot 2x)$ and so our above proposition only holds if R is an integral domain.

Remark: To extend proposition 82(2) to the zero polynomial, we define $\deg(0) = \pm\infty$.

9.2 Polynomials over a Field

Definition. Monic Polynomials: Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is monic if its leading coefficient is 1.

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

Proposition 83: Let $f(x), g(x), h(x) \in F[x]$. Then

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

Proof. Exercise □

Proposition 84: Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

Proof. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then there exists polynomials $u(x), v(x) \in F[x]$ such that $g(x) = f(x)u(x)$ and $f(x) = g(x)v(x)$. Then $f(x) = g(x)v(x) = f(x)u(x)v(x)$. By proposition 82, $\deg f = \deg f + \deg u + \deg v$ which implies $\deg(u) = 0 = \deg(v)$. Thus $g(x) = f(x) \cdot s$ for some $s \in R$. Since $f(x)$ and $g(x)$ are monic, $s = 1$ and we have $f(x) = g(x)$. □

Remark: We recall that for any $a, b \in \mathbb{Z}$ if $a \mid b$ and $b \mid a$ and a, b are positive, then $a = b$. Thus, the set of monic polynomials in $F[x]$ plays the same role as the set of positive integers.

Proposition 85. Division Algorithm for Polynomials: Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$. Then there exists 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 $r(x) = 0$ since $\deg 0 = -\infty$.

Proof. We prove by induction that such $q(x)$ and $r(x)$ exist. Write $m = \deg f$ and $n = \deg g$. If $n < m$, then $g(x) = 0 \cdot f(x) + g(x)$. Suppose $n \geq m$ and the result hold for all $g(x) \in F[x]$ with $\deg g < n$. I.e., we are inducting on the degree, n, of the dividend.

Write $f(x) = a_0 + a_1x + \cdots + a_mx^m$ with $a_m \neq 0$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$. Since F is a field, a_m^{-1} exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_na_m^{-1}x^{n-m}f(x) \\ &= (b_nx^n + b_{n-1}x^{n-1} + \cdots) - b_na_m^{-1}x^{n-m}(a_mx^m + a_{m-1}x^{m-1} + \cdots) \\ &= 0x^n + (b_{n-1} - b_na_m^{-1}a_{m-1})x^{n-1} + \cdots \end{aligned}$$

Since $\deg g_1 < n$, by our inductive hypothesis, there exists $q_1(x), r_1(x) \in F[x]$ such that $g_1(x) = q_1(x)f(x) + r_1(x)$ with $\deg r_1 < \deg f$. Thus

$$\begin{aligned} g(x) &= g_1(x) + b_na_m^{-1}x^{n-m}f(x) \\ &= (q_1(x)f(x) + r_1(x)) + b_na_m^{-1}x^{n-m}f(x) \\ &= \underbrace{(q_1(x) + b_na_m^{-1}x^{n-m})}_{q(x)}f(x) + \underbrace{r_1(x)}_{r(x)} \end{aligned}$$

Now to prove uniqueness, suppose we have

$$g(x) = q_1(x)f(x) + r_1(x) \qquad \text{and} \qquad g(x) = q_2(x)f(x) + r_2(x)$$

Then $r_1(x) - r_2(x) = f(x)(q_2(x) - q_1(x))$. If $q_2 - q_1(x) \neq 0$, we get

$$\deg(r_1 - r_2) = \deg f + \deg(q_2 - q_1) \geq \deg f.$$

This leads to a contradiction since $\deg(r_1 - r_2) < \deg f$. Thus $q_2(x) - q_1(x) = 0$ and hence $r_1(x) - r_2(x) = 0$. It follows that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. □

11/14, lecture 10-1

Proposition 86: Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$ and $g(x) \neq 0$. Then there exists $d(x) \in F[x]$ which satisfies the following conditions:

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

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 (if $f \in X$ with leading coefficient a, then $a^{-1}f \in X$ is monic).

Among all monic polynomials in X, choose $d(x) = u(x)f(x) + v(x)g(x)$ of minimal degree. Then (1) and (4) are satisfied. For (3), if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, since $d(x) = u(x)f(x) + v(x)g(x)$, by proposition 83, $e(x) \mid d(x)$.

It remains to prove (2). By the division algorithm, we may find $q(x), r(x) \in F[x]$ such that $f(x) = q(x)d(x) + r(x)$ with $\deg r < \deg d$. Then

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

Note if $r \neq 0$, let $c \neq 0$ be the leading coefficient of $r(x)$. Since F is a field, c^{-1} exists. The above expression of $r(x)$ shows that $c^{-1}r(x)$ is a monic polynomial of X with $\deg(c^{-1}r(x)) = \deg r < \deg d$ which contradicts the choice of $d(x)$ (since $d(x)$ is the minimal monic polynomial with $d(x) = u(x)f(x) + v(x)g(x)$). Thus $r(x) = 0$ and so $d(x) \mid f(x)$. We may similarly show $d(x) \mid g(x)$. □

Note: Note that if both $d_1(x)$ and $d_2(x)$ satisfies the above conditions, since $d_1(x) \mid d_2(x)$ and $d_2(x) \mid d_1(x)$ and both of them are monic, by proposition 84, we have $d_1(x) = d_2(x)$. We call such $d(x)$ the greatest common divisor of $f(x)$ and $g(x)$, denoted by $d(x) = \gcd(f(x), g(x))$. Thus the greatest common divisor is unique (at least among monic polynomials).

Definition. Irreducible Polynomial: Let F be a field, a polynomial $\ell(x) \neq 0$ in $F[x]$ is irreducible if $\deg \ell \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ with $\ell_1(x), \ell_2(x) \in F[x]$, then $\deg \ell_1 = 0$ and $\deg \ell_2 = \deg \ell$ or $\deg \ell_1 = \deg \ell$ and $\deg \ell_2 = 0$ (recall degree 0 polynomials are units in $F[x]$). Polynomials that are not irreducible are reducible.

Example: If $\ell(x) \in F[x]$ satisfies $\deg \ell = 1$, then $\ell(x)$ is irreducible. (For $\deg \ell = 2$ or 3, see assignment 9).

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

Proof. Suppose $\ell(x) \mid f(x)g(x)$. We consider two cases, if $\ell(x) \mid f(x)$ then we are done, otherwise suppose $\ell(x) \nmid f(x)$. Then $\gcd(\ell(x), f(x)) = 1$. Thus there exists $u(x), v(x) \in F[x]$

such that $1 = u(x)\ell(x) + v(x)f(x)$. Then

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

Since $\ell(x) \mid \ell(x)$ and $\ell(x) \mid f(x)g(x)$, by proposition 83, we have $\ell(x) \mid g(x)$. □

Remark: Let $f_1(x), \ldots, f_n(x) \in F[x]$ and let $\ell(x) \in F[x]$ be irreducible. If $\ell(x) \mid f_1(x) \cdots f_n(x)$, by applying proposition 87 repeatedly, we get $\ell(x) \mid f_i(x)$ for some $1 \leq i \leq n$.

Theorem 88. Unique Factorization Theorem: Let F be a field and let $f(x) \in F[x]$ with $\deg f \geq 1$. Then we can write

$$f(x) = c\ell_1(x) \cdots \ell_m(x)$$

where $c \in F^*$ and $\ell_i(x)$ are monic, irreducible polynomials for $1 \leq i \leq n$. The factorization is unique up to the order of ℓ_i.

Proof. Exercise, see Piazza. □

11/16, lecture 10-2

Proposition 89: 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.

Proof. Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0 \rangle$. If $A \neq \{0\}$, then A contains a monic polynomial (since we can multiply by the inverse of the leading coefficient). Choose $h(x) \in A$ of minimal degree. Then $\langle h(x) \rangle \subseteq A$.

To prove the other inclusion, let $f(x) \in A$. By the division algorithm, we may write $f(x) = q(x)h(x) + r(x)$ with $\deg r < \deg h$. If $r(x) \neq 0$, let $u \neq 0$ be its leading coefficient. Since A is an ideal and $f(x), h(x) \in A$, 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 $\deg(u^{-1}r) < \deg h$, which contradicts the minimality of $\deg h$. Thus, $r(x) = 0$ and $h(x) \mid f(x)$. It follows that $A \subseteq \langle h(x) \rangle$ and so $A = \langle h(x) \rangle$.

Also, if $\langle h(x) \rangle = \langle h'(x) \rangle$, then $h(x) \mid h'(x)$ and $h'(x) \mid h(x)$. If both $h(x)$ and $h'(x)$ are monic, by proposition 84, $h(x) = h'(x)$. □

Exploration: Let $A \neq \{0\}$ be an ideal of $F[x]$. By proposition 89, we can write $A = \langle h(x) \rangle$ for a unique monic polynomial $h(x) \in F[x]$. Suppose that $\deg h = m \geq 1$. Consider the quotient ring $R = F[x]/A$ so that

$$R = \{\overline{f(x)} = f(x) + A : f(x) \in F[x]\} \qquad \text{where} \qquad \overline{f(x)} := f(x) + A.$$

Write $t = \overline{x} = x + A$, then by the division algorithm (write $f(x) = q(x)h(x) + r(x)$ with $\deg r < \deg h = m$, then our cosets are uniquely determined by $r(x)$), we have

$$R = \{\overline{a_0} + \overline{a_1}t + \overline{a_2}t^2 + \cdots + \overline{a_{m-1}}t^{m-1} : a_i \in F\}$$

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

$$R = \{a_0 + a_1t + \cdots + a_{m-1}t^{m-1} : a_i \in F\}$$

Note that in R, we have $a_0 + a_1t + \cdots + a_{m-1}t^{m-1} = b_0 + b_1t + \cdots + b_{m-1}t^{m-1}$ if and only if $a_0 = b_0, a_1 = b_1, \ldots, a_{m-1} = b_{m-1}$ (exercise). So the representation of the elements of R is unique. Finally, in the ring R, we have $h(t) = 0$ (since $h(t) = \overline{h(x)} = 0_R$).

Proposition 90: Let F be a field and $h(x) \in F[x]$ by monic with $\deg h = m \geq 1$. Then the quotient ring $R = F[x]/\langle h(x)\rangle$ is given by

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

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

Proof. See the above exploration. □

Example: In $\mathbb{Z}$, we have $\mathbb{Z}/\langle n\rangle = \mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, which is analogous to proposition 90.

Example: Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By proposition 90, we have

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

In particular, $\langle x^2 + 1\rangle$ is maximal in $\mathbb{R}[x]$.

Proposition 91: Let F be a field and let $h(x) \in F[x]$ be a polynomial 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 $F[x]$.

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

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

($2 \implies 3$) If $h(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$, 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 $g(x) + A = 0 + A$. Without loss of generality, suppose $f(x) + A = 0 + A$. Then $f(x) \in A = \langle h(x) \rangle$. Thus $f(x) = h(x)q(x)$ for some $q(x) \in F[x]$. Thus

$$h(x) = f(x)g(x) = h(x)q(x)g(x)$$

This implies that $q(x)g(x) = 1$ and hence $\deg g = 0$. Similarly, if $g(x) + A = 0 + A$, then $\deg f = 0$. Thus $h(x)$ is irreducible by definition.

($3 \implies 1$) Note that $F[x]/A$ is a commutative ring. Thus to show it is a field, it suffices to find an inverse of any nonzero element. Let $f(x) + A \neq 0 + A$. Then $f(x) \notin A$, i.e., $h(x) \nmid f(x)$. Since $h(x)$ is irreducible and $h(x) \nmid f(x)$, $\gcd(h(x), f(x)) = 1$. By proposition 86, there exist $u(x), v(x) \in F[x]$ such that

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

Thus $(u(x)+A)(f(x)+A) = 1+A$ since $(h(x)+A)(v(x)+A) = (0+A)(v(x)+A) = 0+A$. Hence $f(x)$ is invertible and so $F[x]/A$ is a field. □

Example: Since $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$, we see that $x^2 + 1$ is irreducible in $\mathbb{R}$.

Example: Since $x^3 + x + 1$ has no roots in $\mathbb{Z}_2$, it is irreducible in $\mathbb{Z}_2$. Thus

$$\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle/ \cong \{a_0 + a_1 t + a_2 t^2 : a_i \in \mathbb{Z}_2 \text{ and } t^3 + t + 1 = 0\}$$

is a field of 8 elements. Note that $\mathbb{Z}_8$ is not a field, thus this gives us an "interesting" finite field.

11/18, lecture 10-3

Remark: Given a prime p and $n \in \mathbb{N}$, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$ (the proof of this result is non-trivial), say $\ell(x)$. Then $\mathbb{Z}_p[x]/\langle \ell(x)\rangle$ is a field of order p^n

Remark: Analogies between $\mathbb{Z}$ and $F[x]$:

	$\mathbb{Z}$	$F[x]$
Elements	m	$f(x)$
Size	$\lvert m \rvert$	$\deg f$
Units	± 1	F^*
"Positives"	$(\mathbb{Z} \setminus \{0\})/\{\pm 1\} \cong \mathbb{N}$	$(F[x] \setminus \{0\})/F^* \cong M$
UFT	$m = \pm 1 p_1^{\alpha_1} \cdots p_n^{\alpha_n}$	$f = c\ell_1^{\alpha_1} \cdots \ell_n^{\alpha_n}$
	p_i is prime	$c \in F^*$, ℓ_i is monic and irreducible
Ideals	$\langle n \rangle$ (unique if $n \in \mathbb{N}$)	$\langle h(x) \rangle$ (unique if $h(x)$ is monic).
Quotient Rings	$\mathbb{Z}/\langle n \rangle$ is a field iff n is prime	$F[x]/\langle h(x) \rangle$ is a field iff $h(x)$ is irreducible.

where $M = \{f(x) \in F[x] : f(x) \text{ is monic}\}$. We should also note that both have a division algorithm.

Chapter 10 Integral Domains

10.1 Irreducibles and Primes

Definition. Divisibility: Let R be an integral domain and $a, b \in R$. We say a divides b, denoted by $a|b$, if $b = ca$ for some $c \in R$.

Proposition 92: Let R be an integral domain. For $a, b \in R$, the following are equivalent:

1. $a \mid b$ and $b \mid a$.
2. $a = ub$ for some unit $u \in R$.
3. $\langle a \rangle = \langle b \rangle$.

Proof. Exercise, see Piazza. □

Definition. Association: Let R be an integral domain. For $a, b \in R$, we say a is associated to b, denoted by $a \sim b$, if $a \mid b$ and $b \mid a$. By proposition 92, $\sim$ is an equivalence relation. More precisely

1. $a \sim a$ for all $a \in R$.
2. If $a \sim b$, then $b \sim a$.
3. If $a \sim b$ and $b \sim c$, then $a \sim c$.

Moreover, one can show (exercise)

1. If $a \sim a'$ and $b \sim b'$, then $ab \sim a'b'$.
2. If $a \sim a'$ and $b \sim b'$, then $a \mid b$ if and only if $a' \mid b'$.

Example: Let $R = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}$, which is an integral domain. Note that $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$. Thus $2 + \sqrt{3}$ is a unit in R. Since $(2 + \sqrt{3}) \cdot \sqrt{3} = 3 + 2\sqrt{3}$. Thus $3 + 2\sqrt{3} \sim \sqrt{3}$ in R.

Definition. Irreducible Element: Let R be an integral domain. We say $p \in R$ is irreducible if $p \neq 0$ is not a unit, and if $p = ab$ with $a, b \in R$, then either a or b is a unit. An element that is not irreducible is reducible.

Example: Let $R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ and let $p = 1 + \sqrt{-5}$. We claim that p is irreducible in R. For $d = m + n\sqrt{-5}$, the norm of d is defined to be

$$N(d) = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}$$

(Note the norm has a clear analogy to the modulus for complex numbers given by $|a + bi| = (a + bi)(a - bi)$.) One can check (see assignment 10):

- $N(ab) = N(a)N(b)$.
- $N(d) = 1$ if and only if d is a unit.
- If $N(\ell)$ is a prime then ℓ is irreducible.

Now suppose that $p = 1 + \sqrt{-5} = ab$ with $a, b \in R$. Note that $N(p) = 6 = N(a)N(b)$. Note the only factorization of 6 is $6 = 1 \cdot 6$ or $6 = 2 \cdot 3$. If $N(m + n\sqrt{-5}) = m^2 + 5n^2 = 2$, then $n = 0$ and thus $m^2 = 2$, which is not possible. Thus $N(m + n\sqrt{-5}) \neq 2$. Similarly $N(m + n\sqrt{-5}) \neq 3$. Thus we have either $N(a) = 1$ or $N(b) = 1$, i.e., either a or b is a unit. Thus p is irreducible.

11/21, lecture 11-1

Proposition 93: Let R be an integral domain and let $0 \neq p \in R$ with p not being a unit. The following are equivalent:

1. p is irreducible.
2. If $d \mid p$, then $d \sim 1$ or $d \sim p$.
3. If $p \sim ab$ in R, then $p \sim a$ or $p \sim b$.
4. If $p = ab$ in R, then $p \sim a$ or $p \sim b$.

As a consequence, we see that if $p \sim q$, then p is irreducible if and only if q is irreducible.

Proof. ($1 \implies 2$) If $p = da$ for some $a \in R$, by (1) either d or a is a unit. Then $d \sim 1$ or $d \sim p$.

($2 \implies 3$) If $p \sim ab$, then $b \mid p$. By (2), either $b \sim 1$ or $b \sim p$. In the first case, we get $p \sim a$.

($3 \implies 4$) Clearly true.

($4 \implies 1$) If $p = ab$, then by (4), $p \sim a$ or $p \sim b$. If $p \sim a$, write $a = up$ for some unit u. Then $p = ab = (up)b = pub$. Since R is an integral domain and $p \neq 0$, we have $ub = 1$, i.e., b is a unit. Similarly, $p \sim b$ implies that a is a unit. Thus (1) follows. □

Definition. Prime Element: Let R be an integral domain and $p \in R$. We say p is a prime if $p \neq 0$ is not a unit, and if $p \mid ab$ with $a, b \in R$, then $p \mid a$ or $p \mid b$.

Remark: If $p \sim q$, then p is prime if and only if q is prime. Also, by induction, if p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.

Proposition 94: Let R be an integral domain and $p \in R$. If p is a prime, then p is irreducible.

Proof. Let $p \in R$ be a prime. If $p = ab$ in R, then $p \mid a$ or $p \mid b$ since p is a prime. If $p \mid a$, write $a = dp$ for some $d \in R$. Since R is commutative, we have $a = dp = d(ab) = a(db)$. Since $0 \neq a$ and R is an integral domain, we have $db = 1$ and thus b is a unit with inverse d. Similarly, if $p \mid b$, then a is a unit. It follows that p is irreducible. □

Example: The converse of proposition 94 is false. Consider for instance, $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5} \in R$. We have seen that p is irreducible in R. We claim that p is not a prime in R.

Note that $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. If p is a prime, since $p \mid 2 \cdot 3$ then $p \mid 2$ or $p \mid 3$. Suppose that $p \mid 2$, say $2 = qp$ for some $q \in R$. It follows that $4 = N(2) = N(q)N(p) = N(q) \cdot 6$ which is not possible, since we know that $N(q) \in \mathbb{Z}$ and $6 \nmid 4$ in $\mathbb{Z}$. Similarly, if $p \mid 3$ is not possible, since $N(p) = 6 \nmid 9 = N(3)$. Thus p is not a prime.

Note: The following are good exercises:

1. Construct another irreducible element that is not a prime.
2. Given a prime $p \in \mathbb{Z}$, i.e., $p = (\pm 1)(\pm p)$ is the only factorization of p, try to think what is needed to prove Euclid's Lemma that $p \mid ab$ implies $p \mid a$ or $p \mid b$?

10.2 Ascending Chain Conditions

Definition. Ascending Chain Conditions: An integral domain R is said to satisfy the ascending chain conditions on principal ideals (ACCP) if for any ascending chain of principal ideals in R, $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$, then there exists an integer $n \in \mathbb{N}$ such that $\langle a_n \rangle = \langle a_{n+1} \rangle = \langle a_{n+2} \rangle = \cdots$.

Example: We claim $\mathbb{Z}$ satisfies ACCP.

Proof. If $\langle a_1 \rangle \subseteq \langle a_3 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$ in $\mathbb{Z}$, then $a_2 \mid a_1, a_3 \mid a_2, a_4 \mid a_3, \ldots$. Taking absolute values gives $|a_1| \geq |a_2| \geq |a_3| \geq \cdots$. Since each $|a_i| \geq 0$ is an integer, we get $|a_n| = |a_{n+1}| = \cdots$ for some n. It implies that $a_{i+1} = \pm a_i$ for all $i \geq n$. Thus $\langle a_i \rangle = \langle a_{i+1} \rangle$ for all $i \geq n$. □

11/23, lecture 11-2

Example: Consider $R = \langle n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$ the set of polynomials in $\mathbb{Q}[x]$ whose constant term is in $\mathbb{Z}$. Then R is an integral domain (exercise), but $\langle x \rangle \subsetneq \langle \frac{1}{2}x \rangle \subsetneq \langle \frac{1}{4}x \rangle \subsetneq \langle \frac{1}{8}x \rangle \subsetneq \cdots$. Thus R does not satisfy ACCP, as this chain does not have a constant tail.

Theorem 95: Let R be an integral domain satisfying ACCP. If $0 \neq a \in R$ is not a unit, then a is a product of irreducible elements of R.

Proof. By way of contradiction, suppose that there exists a nonunit $0 \neq a \in R$ which is not a product of irreducible elements. Since a is not irreducible, by proposition 93, we may write

$a = x_1a_1$ with $a \nsim x_1$ and $a \nsim a_1$. Note that at least one of x_1 and a_1 are not a product of irreducible elements (if both of them are, so is a).

Without loss of generality, suppose a_1 is not a product of irreducible elements. Then as before, we can write $a_1 = x_2a_2$ with $a_1 \nsim x_2$ and $a_1 \nsim a_2$ and where a_2 is not a product of irreducible elements. This process may be continued infinitely and we have

$$\langle a\rangle \subseteq \langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots$$

Since $a \nsim a_1, a_1 \nsim a_2, \ldots$, by proposition 92 we have

$$\langle a\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots .$$

This is a contradiction of the ACCP condition on R. Thus all non-unit $0 \neq a \in R$ are products of irreducible elements of R. □

Theorem 96: If R is an integral domain satisfying ACCP, so is $R[x]$.

Proof. By way of contradiction, suppose that $R[x]$ does not satisfy ACCP. Then there exists

$$\langle f_1\rangle \subsetneq \langle f_2\rangle \subsetneq \langle f_3\rangle \subsetneq \cdots$$

in $R[x]$. Thus we have $\cdots \mid f_3 \mid f_2 \mid f_1$. Let a_i be the leading coefficient of f_i. Since $f_{i+1} \mid f_i$, we have $a_{i+1} \mid a_i$ for all i. Thus

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots$$

in R. Since R satisfies ACCP, we have $\langle a_n\rangle = \langle a_{n+1}\rangle = \langle a_{n+2}\rangle = \cdots$ for some $n \geq 1$. We see then that $a_n \sim a_{n+1} \sim a_{n+2} \sim \cdots$ by proposition 92. For $m \geq n$, let $f_m = gf_{m+1}$ for some $g(x) \in R[x]$ (since $f_{m+1} \mid f_m$). If b is the leading coefficient of g, then we get $a_m = ba_{m+1}$. Since $a_m \sim a_{m+1}$, we must have that b is a unit in R (again by proposition 92). Since $\langle f_m\rangle \subsetneq \langle f_{m+1}\rangle$, $g(x)$ is not a unit as otherwise $f_m \sim f_{m+1}$. Thus $g(x) \neq b$ and $\deg g \geq 1$.

Thus by proposition 82, it implies that $\deg f_m > \deg f_{m+1}$. This is true for all $m \geq n$. Thus we have

$$\deg f_n > \deg f_{n+1} > \deg f_{n+2} > \cdots$$

which leads to a contradiction since $\deg f_i \geq 0$. Thus $R[x]$ satisfies the ACCP. □

Example: Since $\mathbb{Z}$ satisfies ACCP, so does $\mathbb{Z}[x]$. (So does $\mathbb{Z}[x, y]$, polynomials in two variables over $\mathbb{Z}$.)

10.3 Unique Factorization Domains and Principle Ideal Domains

Definition. Unique Factorization Domain: An integral domain R is called a unique factorization domain (UFD) if it satisfies the following conditions:

1. If $0 \neq a \in R$ is not a unit, then a is a product of irreducible elements in R.

2. If $p_1p_2\cdots p_r \sim q_1q_2\cdots q_s$, where p_i and q_j are irreducible for all i, j, then $r = s$ and after possibly rearranging, $p_i \sim q_i$ for all $1 \leq i \leq r$.

Example: $\mathbb{Z}$ and $F[x]$ (where F is a field) are unique factorization domains.

Example: Every field is a unique factorization domain, since it has non nonzero nonunit elements.

Proposition 97: Let R be a unique factorization domain and $p \in R$. If p is irreducible, then p is prime.

Proof. Let $p \in R$ be irreducible. If $p \mid ab$ with $a, b \in R$, write $ab = pd$ for some $d \in R$. Since R is a UFD, we can factor a, b and d into irreducible elements. Say,

$$a = p_1p_2\cdots p_k, \qquad b = q_1q_2\cdots q_\ell, \qquad d = r_1r_2\cdots r_m$$

(here we allow k, ℓ, or m to be zero to cover the case that a, b or d is a unit). Since $pd = ab$, we write

$$pr_1r_2\cdots r_m = p_1p_2\cdots p_kq_1q_2\cdots q_\ell.$$

Since p is irreducible, by proposition 93, it implies $p \sim p_i$ for some i or $p \sim q_j$ for some j. Thus $p \mid a$ or $p \mid b$, as desired. □

11/25, lecture 11-3

Example: Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5} \in R$. We have seen before that p is irreducible, but not prime. By proposition 97, R is not a UFD. For example, $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$ where $1 \pm \sqrt{-5}, 2, 3$ are irreducible (exercise). However, $(1+\sqrt{-5}) \not\sim 2$ and $(1+\sqrt{-5}) \not\sim 3$. Since $N(1+\sqrt{-5}) = 6$ while $N(2)$ and $N(3) = 9$.

Example: We claim that $R = \mathbb{Z}[\sqrt{-5}]$ satisfies ACCP.

Proof. If $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots$ in R, then $a_2 \mid a_1, a_3 \mid a_2, \ldots$. Taking their norms gives $N(a_1) \geq N(a_2) \geq \cdots$. Since $N(a_i) \geq 0$ is an integer, we get $N(a_n) = N(a_{n+1}) = \cdots$ for some $n \in \mathbb{N}$. Since $N(d) = 1$ if and only if d is a unit in R, it follows that $a_{i+1} \sim a_i$ for all $i \geq n$. Thus $\langle a_i\rangle = \langle a_{i+1}\rangle$ for all $i \geq n$. □

Definition. Greatest Common Divisor: Let R be an integral domain and $a, b \in R$. We say $d \in R$ is a greatest common divisor (note that it's no longer unique) of a, b, denoted by $d = \gcd(a, b)$, if it saatisfies the following conditions:

1. $d \mid a$ and $d \mid b$

2. If $e \in R$ with $e \mid a$ and $e \mid b$, then $e \mid d$

One can prove

Proposition 98: Let R be a UFD and $a, b \in R \setminus \{0\}$. If $p_1, p_2, \ldots, p_k$ are the non-associated primes dividing a and b, say

$$a \sim p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad b \sim p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

with $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$ for all $1 \leq i \leq k$. Then

$$\gcd(a, b) \sim p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

Proof. Exercise. $\square$

Remark: If R is a UFD with $d, a_1, \ldots, a_m \in R$, we have

$$\gcd(da_1, da_2, \ldots, da_m) \sim d \gcd(a_1, a_2, \ldots, a_m)$$

Theorem 99. Nagata Criterion: Let R be an integral domain. The following are equivalent:

1. R is a UFD
2. R satisfies ACCP and $\gcd(a, b)$ exists for all nonzero $a, b \in R$
3. R satisfies ACCP and every irreducible element in R is prime

Proof. ($1 \implies 2$) By proposition 98, $\gcd(a, b)$ exists. By way of contradiction, suppose that there exists $0 \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$ in R, since $\langle a_1 \rangle \neq R$, a_1 is not a unit. Write $a_1 \sim p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are non-associated primes and $k_i \in \mathbb{N}$. Since $a_i \mid a_1$ for all i, we have $a_i \sim p_1^{d_{i,1}} \cdots p_r^{d_{i,r}}$ for $0 \leq d_{i,j} \leq k_j$ for all $1 \leq j \leq r$. Thus there are only finitely many non-associated choices for a_i and so there exists $m \neq n$ with $a_m \sim a_n$. This implies $\langle a_m \rangle = \langle a_n \rangle$, a contradiction. Thus R satisfies ACCP.

($2 \implies 3$) Let $p \in R$ be irreducible and suppose $p \mid ab$. By (2), let $d = \gcd(a, p)$. Thus $d \mid p$, and since p is irreducible, we have $d \sim p$ or $d \sim 1$. In the first case, since $d \sim p$ and $d \mid a$, we get $p \mid a$. In the second case, since $d = \gcd(a, p) \sim 1$, then $\gcd(ab, pb) \sim b$. Since $p \mid ab$ and $p \mid pb$, we have $p \mid \gcd(ab, pb)$, i.e., $p \mid b$.

($3 \implies 1$) If R satisfies ACCP, by theorem 95, every nonunit $0 \neq a \in R$ is a product of irreducible elements of R. Thus is suffices to show such factorization is unique. Suppose we have $p_1 p_2 \cdots p_r \sim q_1 q_2 \cdots q_s$ where p_i, q_j are irreducible. Since p_1 is prime, then $p_1 \mid q_j$ for some j, say q_1. By proposition 93, we have $p_1 \sim q_1$. Similarly, $p_2 \sim q_2$. Continuing in this way, we see have that $r = s$ and $p_r \sim q_r$. $\square$

11/28, lecture 12-1

Definition. Principal Ideal Domain: An integral domain R is said to be a principal ideal domain (PID) if every ideal is principal. That is, every ideal of the form $\langle a\rangle = aR$ for some $a \in R$.

Example: $\mathbb{Z}$ and $F[x]$ (where F is a field) are PIDs.

Example: A field F is a PID since the only ideals in F are $\{0\} = \langle 0\rangle$ and $F = \langle 1\rangle$.

Proposition 100: Let R be a be a PID and let $a_1, \ldots, a_n \in R$ be nonzero elements of R. Then $d \sim \gcd(a_1, \ldots, a_n)$ exists and there exist $r_1, \ldots, r_n \in R$ such that

$$\gcd(a_1, \ldots, a_n) = r_1a_1 + \cdots + r_na_n.$$

Proof. Let $A = \{r_1a_1+\cdots+r_na_n : r_i \in R\} = \langle a_1, \ldots, a_n\rangle$ be an ideal of R. Since R is a PID, there exists $d \in R$ such that $A = \langle d\rangle$. Thus $d = r_1a_1 + \cdots + r_na_n$ for some $r_1, \ldots, r_n \in R$. We claim that $d \sim \gcd(a_1, \ldots, a_n)$.

Since $A = \langle d\rangle$ and $a_i \in A$, we have $d \mid a_i$ for all $1 \leq i \leq n$. Also, if $r \mid a_i$ for all $1 \leq i \leq n$, then $r \mid (r_1a_1 + \cdots + r_na_n)$, i.e., $r \mid d$. By the definition of the GCD, we have that $d \sim \gcd(a_1, \ldots, a_n)$. □

Theorem 101: Every PID is a UFD.

Proof. If R is a PID, by theorem 99 and proposition 100, it suffices to show that R satisfies ACCP. Suppose we have $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots$ in R, let $A = \langle a_1\rangle \cup \langle a_2\rangle \cup \langle a_3\rangle \cup \cdots$. Then A is an ideal (exercise). Since R is a PID, we can write $A = \langle a\rangle$ for some $a \in R$. Thus, we must have $a \in \langle a_n\rangle$ for some $n \in \mathbb{N}$ and hence

$$\langle a\rangle \subseteq \langle a_n\rangle \subseteq \langle a_{n+1}\rangle \subseteq \cdots \subseteq \langle a\rangle.$$

Thus, $\langle a_n\rangle = \langle a_{n+1}\rangle = \cdots = \langle a\rangle$, i.e., R satisfies ACCP, as desired. Hence R is a UFD. □

Theorem 102: Let R be a PID. If $0 \neq p \in R$ is not a unit, the following are equivalent:

1. p is a prime
2. $R/\langle p\rangle$ is a field
3. $R/\langle p\rangle$ is an integral domain.

By propositions 77 and 78, we see from (2) and (3) that in a PID, every nonzero prime ideal is maximal

Proof. $(2 \implies 3)$ every field is an integral domain.

$(3 \implies 1)$ Suppose $p \mid ab$ with $a, b \in R$. Then

$$(a + \langle p\rangle)(b + \langle p\rangle) = ab + \langle p\rangle = 0 + \langle p\rangle$$

in $R/\langle p\rangle$. Since $R/\langle p\rangle$ is an integral domain, we have $a+\langle p\rangle = 0+\langle p\rangle$ or $b+\langle p\rangle = 0+\langle p\rangle$. It follows that either $p \mid a$ or $p \mid b$. Thus p is a prime.

($1 \implies 2$) Consider $0 \neq x = a+\langle p\rangle$ in $R/\langle p\rangle$. Then $a \notin \langle p\rangle$ and thus $p \nmid a$. Consider $A = \{ra+sp : r,s \in R\}$ which is an ideal of R. Since R is a PID, we have $A = \langle d\rangle$ for some $d \in R$. Since $p \in A$, we have $d \mid p$. Since p is prime and thus irreducible, we have $d \sim p$ or $d \sim 1$. If $d \sim p$, then we have $\langle p\rangle = \langle d\rangle = A$. Since $a \in A$, this implies $p \mid a$, which is a contradiction. Thus we have $d \sim 1$. It follows that $A = \langle 1\rangle = R$. In particular, $1 \in A$, say $1 = ab + cp$ for some $b, c \in R$. If $y = b+\langle p\rangle$ in $R/\langle p\rangle$, then

$$xy = (a+\langle p\rangle)(b+\langle p\rangle) = ab+\langle p\rangle = 1-cp+\langle p\rangle = 1+\langle p\rangle = 1_{R/\langle p\rangle}$$

in $R/\langle p\rangle$, since clearly $p \mid cp$. Thus $R/\langle p\rangle$ is a field, as desired □

Remark: In a PID, an ideal is maximal if and only if it is a prime ideal (in general we only have that maximal ideals are prime ideals). In a UFD, an element is prime if and only if it is irreducible (in general we only have that prime elements are irreducible).

Note: Note that we have

$$\underbrace{\text{Rings}}_{\mathsf{M}_n(R)} \supsetneq \underbrace{\text{Commutative rings}}_{\mathbb{Z}_n \text{ for composite } n} \supsetneq \underbrace{\text{Integral domain}}_{\{n+xf\,:\,n\in\mathbb{Z}, f\in\mathbb{Q}[x]\}} \supsetneq \underbrace{\text{ACCP}}_{\mathbb{Z}[\sqrt{-5}]} \supsetneq \underbrace{\text{UFDs}}_{\mathbb{Z}[x]} \supsetneq \underbrace{\text{PIDs}}_{\mathbb{Z}} \supsetneq \underbrace{\text{Fields}}_{\mathbb{Q}}$$

For each type of ring, the ring described underneath is of that type, but not of the next type. E.g., $\mathsf{M}_n(R)$ is a ring, but is not a commutative ring.

Example: We claim that $\mathbb{Z}[x]$ is not a PID.

Proof. Consider $A = \{2n + xf(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ which is an ideal of $\mathbb{Z}[x]$ (exercise). Suppose $A = \langle g(x)\rangle$ for some $g(x) \in \mathbb{Z}[x]$. Then $g(x) \mid 2$. It follows that $g(x) \sim 1$ or $g(x) \sim 2$ and thus $A = \mathbb{Z}[x]$ (but, for instance, $1 \notin A$) or $A = \langle 2\rangle$ (but, for instance, $2+x \notin A$). Both are not possible, thus $\mathbb{Z}[x]$ is not a PID. □

Remark: Note that $\mathbb{Z}[x]$ is a UFD, but we need section 10.4 to prove this.

11/30, lecture 12-2

10.4 Gauss' Lemma

Example: Note that the fraction field of $\mathbb{Z}$ is $\mathbb{Q}$. Consider $2x+4$ in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

- Since $\deg(2x+4) = 1$, we see $2x+4$ is irreducible in $Q[x]$.
- Since $2x+4 = 2(x+2)$ and 2 is not a unit, we see $2x+4$ is reducible in $\mathbb{Z}[x]$.

Definition. Content: If R is a UFD and $0 \neq f(x) \in R[x]$, a greatest common divisor of the nonzero coefficients of $f(x)$ is called a content of $f(x)$ and is denoted by $c(f)$. If $c(f) \sim 1$, we say $f(x)$ is a primitive polynomial.

Example: In $\mathbb{Z}[x]$

$$c(6 + 10x^2 + `15x^3) \sim \gcd(6, 10, 15) \sim 1 \implies \text{primitive}$$
$$c(6 + 9x^2 + `15x^3) \sim \gcd(6, 9, 15) \sim 3 \implies \text{not primitive}$$

Lemma 103: Let R be a UFD and $0 \neq f(x) \in R[x]$. Then

1. $f(x)$ can be written as $f(x) = c(f)f_1(x)$ where $f_1(x)$ is primitive.
2. If $0 \neq b \in R$, then $c(bf) \sim bc(f)$.

Proof. 1. For $f(x) = a_m x^m + \cdots + a_1 x + a_0 x \in R[x]$, let $c = c(f) \sim \gcd(a_0, a_1, \ldots, a_m)$. Write $a_i = cb_i$ for some $b_i \in R$ for all $0 \leq i \leq m$. Then $f(x) = cf_1(x)$ where $f_1(x) = b_m x^m + \cdots b_1 x + b_0$. Thus

$$c \sim \gcd(a_0, a_1, \ldots, a_m) \sim \gcd(cb_0, cb_1, \ldots, cb_m) \sim c \gcd(b_0, b_1, \ldots, b_m)$$

Thus $\gcd(b_0, b_1, \ldots, b_m) \sim 1$ and hence f_1 is primitive.

2. Exercise. □

Lemma 104: Let R be a UFD and let $\ell(x) \in R[x]$ be irreducible with $\deg \ell \geq 1$. Then $c(\ell) \sim 1$.

Proof. By lemma 103, write $\ell(x) = c(\ell)\ell_1(x)$ with $\ell_1(x)$ being primitive. Since $\ell(x)$ is irreducible, either $c(\ell)$ or $\ell_1(x)$ is a unit. Since $\deg \ell_1 = \deg \ell \geq 1$, we see ℓ_1 is not a unit. Thus $c(\ell) \sim 1$. □

Theorem 105. Gauss's Lemma: Let R be a UFD. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then $c(fg) \sim c(f)c(g)$. In particular, the product of primitive polynomials is primitive.

Proof. Let $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$ where f_1 and g_1 are primitive.. Then, by lemma 103,

$$c(fg) \sim c\big(c(f)f_1\, c(g)g_1\big) \sim c(f)c(g)c(f_1 g_1)$$

Thus it suffices to shows that $f_1(x)g_1(x)$ is primitive if $c(f_1) \sim 1$ and $c(g_1) \sim 1$. By way of contradiction, suppose f_1 and g_1 are primitive but $f_1 g_1$ is not primitive. Since R is a UFD, there exists a prime p dividing each coefficient of $f_1(x)g_1(x)$. Write $f_1(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g_1(x) = b_0 + b_1 x + \cdots + b_n x^n$. Since $f_1(x)$ and $g_1(x)$ are primitive, p does NOT divide every a_i or every b_j. Thus there exists $k, s \in \mathbb{N} \cup \{0\}$ such that

1. $p \nmid a_k$, but $p \mid a_i$ for $0 \leq i < k$

2. $p \nmid b_s$, but $p \mid b_j$ for $0 \leq j < s$

Note the coefficient of x^{k+s} in $f(x)g(x)$ is

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

Because of (1) and (2), p divides all $a_i b_j$ with $i + j = k + s$, except $a_k b_s$. In particular, we see that $p \mid a_i b_{k+s-i}$ since $p \mid a_i$ for all $0 \leq i < k$, and similarly $p \mid a_{k+s-j} b_j$ since $p \mid b_j$ for all $0 \leq j < s$. However, $p \nmid a_k b_s$ since $p \nmid a_k$ and $p \nmid b_s$. It follows that $p \nmid c_{k+s}$, a contradiction. Thus $f_1(x)g_1(x)$ is primitive. □

Theorem 106: Let R be UFD whose field of fraction is F. Regard $R \subseteq F$ as a subring of F as usual. If $\ell(x) \in R[x]$ is irreducible in $R[x]$, $\ell(x)$ is irreducible in $F[x]$.

Proof. Let $\ell(x) \in R[x]$ be irreducible. Suppose $\ell(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$. If a and b are the products of the denominators of the coefficients of $g(x)$ and $h(x)$ respectively, then $g_1(x) = ag(x) \in R[x]$ and $h_1(x) = bh(x) \in R[x]$. Note that $ab\ell(x) = g_1(x)h_1(x)$ is a factorization in $R[x]$. Since $\ell(x)$ is irreducible in $R[x]$, by lemma 104, $c(\ell) \sim 1$. Then, by Gauss' Lemma,

$$ab \sim abc(\ell) \sim c(ab\ell(x)) \sim c(g_1 h_1) \sim c(g_1)c(h_1) \qquad (*)$$

Write $g_1(x) = c(g_1)g_2(x)$ and $h_1(x) = c(h_1)h_2(x)$ where $g_2(x)$ and $h_2(x)$ are primitive in $R[x]$. Thus,

$$ab\ell(x) = g_1(x)h_1(x) = c(g_1)c(h_1)g_2(x)h_2(x)$$

By (*), we have $\ell(x) \sim g_2(x)h_2(x)$ in $R[x]$ since $ab \sim c(g_1)c(h_1)$. Now, since $\ell(x)$ is irreducible in $R[x]$, it follows that $h_2(x) \sim 1$ or $g_2(x) \sim 1$. If $g_2(x) \sim 1$ in $R[x]$, then

$$ag(x) = g_1(x) = c(g_1)g_2(x) = c(g_1)u$$

for some unit $u \in R^*$. Thus $g(x) = a^{-1}c(g_1)u$ is a unit in $F[x]$ since for all $0 \neq r \in R$, we have that $r \in F^*$. Similarly, if $h_2 \sim 1$ in R, we can show that $h(x)$ is a unit in $F[x]$. Thus $\ell(x) = g(x)h(x)$ in $F[x]$ implies that either $g(x)$ or $h(x)$ is a unit in $F[x]$. Thus, by definition $\ell(x)$ is irreducible in $F[x]$ □

12/02, lecture 12-3

Remark: We see from the proof of theorem 106 that if $f(x) \in R[x]$ admits a factorization in $F[x]$ as $g(x)h(x)$, then by Gauss' Lemma, there exists $\tilde{g}(x), \tilde{h}(x) \in R[x]$ such that $f(x) = \tilde{g}(x)\tilde{h}(x)$. For example,

$$2x^2 + 7x + 3 = (x + \tfrac{1}{2})(2x + 6) = (2x + 1)(x + 3)$$

Remark: The converse of theorem 106 is false. For example, $2x + 4$ is irreducible in $\mathbb{Q}[x]$, but $2x + 4 = 2(x + 2)$ is reducible in $\mathbb{Z}[x]$.

Proposition 107: Let R be UFD whose field of fractions is F. Regard $R \subseteq F$ as a subring of F. Let $f(x) \in R[x]$ with $\deg f \geq 1$. The following are equivalent:

1. $f(x)$ is irreducible in $R[x]$
2. $f(x)$ is primitive (in $R[x]$) and irreducible in $F[x]$

Proof. ($1 \implies 2$) Follows immediately from lemma 104 and theorem 106.

($2 \implies 1$) By way of contradiction, suppose that $f(x)$ is primitive and irreducible in $F[x]$, but $f(x)$ is reducible in $F[x]$. Then the non-trivial factorization of $f(x)$ in $R[x]$ must be of the form $f(x) = dg(x)$ with $d \in R$ and $d \nsim 1$. This is since, if $f(x) = g(x)h(x)$ with $\deg g \geq 1$ and $\deg h \geq 1$, then since $R[x] \subseteq F[x]$ this would provide a non-trivial factorization in $F[x]$. Since $d \mid f(x)$ and $d \nsim 1$, we see d must divide each coefficient of $f(x)$, which contradicts the fact that $f(x)$ is primitive (since $d \nsim 1$). Thus $f(x)$ is irreducible in $R[x]$. □

Theorem 108: If R is a UFD, the polynomial ring $R[x]$ is also a UFD.

Proof. Note, since R is a UFD it satisfies ACCP, then by theorem 96 $R[x]$ also satisfies ACCP. Hence to prove $R[x]$ is a UFD, it suffices to show every irreducible element $\ell(x) \in R[x]$ is prime by theorem 99.

Let $\ell(x) \mid f(x)g(x)$ in $R[x]$. We will prove either $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$. Suppose $\deg \ell = 0$ so that ℓ is a constant. Then $\ell \mid f(x)g(x)$ implies $\ell \mid c(fg) = c(f)c(g)$. Since ℓ is prime in R, we have $\ell \mid c(f)$ or $\ell \mid c(g)$. So $\ell \mid f(x)$ or $\ell \mid g(x)$ respectively. Assume $\deg \ell \geq 1$. We claim it suffices to show that if $\ell(x) \mid f_1(x)g_1(x)$ where $f_1(x)$ and $g_1(x)$ are primitive, then $\ell(x) \mid f_1(x)$ or $\ell(x) \mid g_1(x)$.

We now prove our claim. Since $\ell(x) \mid f(x)g(x)$ in $R[x]$ (where $f(x)$ and $g(x)$ are not necessarily primitive), we have $\ell(x)h(x) = f(x)g(x)$ for some $h(x) \in R[x]$. By lemma 103, write $f(x) = c(f)f_1(x)$, and $g(x) = c(g)g_1(x)$, and $h(x) = c(h)g_1(h)$, where $f_1(x)$, $g_1(x)$, and $h_1(x)$ are primitive in $R[x]$. By lemma 104 (this is why we need $\deg \ell \geq 1$), we see $c(\ell) \sim 1$. It follows that $c(h) \sim c(f)c(g)$. Since $c(h)h_1(x)\ell(x) = c(f)c(g)f_1(x)g_1(x)$, it follows that $h_1(x)\ell(x) \sim f_1(x)g_1(x)$. By the assumption of our claim we have $\ell(x) \mid f_1(x)$ or $\ell(x) \mid g_1(x)$. Thus $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$, as desired.

Thanks to our claim, we now assume that $\ell(x) \mid f(x)g(x)$ where $f(x)$ and $g(x)$ are primitive in $R[x]$. Let F denote the field of fractions of R and consider $R \subseteq F$ as a subring of F. Then we have $\ell(x) \mid f(x)g(x)$ in $F[x]$. Since $\ell(x) \in R[x]$ is irreducible, by theorem 106 $\ell(x)$ is irreducible in $F[x]$. By proposition 87, we have $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$ in $F[x]$. Suppose that $\ell(x) \mid f(x)$ in $F[x]$, say $f(x) = \ell(x)k(x)$ for some $k(x) \in F[x]$. If $d \in R$ is the product of all the denominators of nonzero coefficients of $k(x)$, then $k_0(x) = dk(x) \in R[x]$, and we have $df(x) = d\ell(x)k(x) = k_0(x)\ell(x)$. Since $f(x)$ is primitive and $\ell(x)$ is irreducible (so that $c(\ell) \sim 1$ by lemma 104), we have

$$d \sim c(df) \sim c(k_0\ell) \sim c(k_0)c(\ell) \sim c(k_0)$$

If we write $k_0(x) = c(k_0)k_1(x)$ with $k_1(x) \in R[x]$, then $df(x) = k_0(x)\ell(x) = c(k_0)k_1(x)\ell(x)$. Since $d \sim c(k_0)$, it follows that $f(x) \sim k_1(x)\ell(x)$. Thus $\ell(x) \mid f(x)$ in $R[x]$. Similarly, if $\ell(x) \mid g(x)$ in $F[x]$, then we can show that $\ell(x) \mid g(x) \in R[x]$. It follows that $\ell(x)$ is prime and thus $R[x]$ is a UFD. □

Definition. Multivariable Polnomial Ring: Let R be a UFD and $x_1, \ldots, x_n$ be n commuting variables, i.e., $x_i x_j = x_j x_i$ for all $i \neq j$. Define the ring $R[x_1, \ldots, x_n]$ of polynomials in n variables by $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ for $n \geq 1$.

Corollary 109: If R is a UFD, then for all $n \in \mathbb{N}$ the polynomial ring in n variables $R[x_1, \ldots, x_n]$ is also a UFD.

Proof. Immediate consequence of theorem 108. $\square$

Corollary 110: $\mathbb{Z}[x]$ and $\mathbb{Z}[x_1, \ldots, x_n]$ are UFDs.

Proof. Follows from theorem 108 and corollary 109 since $\mathbb{Z}$ is a UFD. $\square$

Index