Math 511A Algebra
University Of Arizona Mathematics
Fall 2010

Lectured by Doctor Ana-Maria Castravet (noni@math.arizona.edu)
Typeset by Alex Tao (taolapkei@math.arizona.edu)

Last Update: January 11, 2011

Contents

Reading: Dummit and Foote, Abstract Algebra, Third Edition

Algebra is the study of abstract structures, e.g. groups, rings, modules, vector space etc.

1 Group Theory

1.1 Review of Groups

Definition 1.1.1
A group is a set G together with a binary operation $*$:

$$\begin{aligned} G \times G &\to G \\ (a, b) &\to a * b \end{aligned}$$

such that

(i) $*$ is associative: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$

(ii) $\exists e =$ identity element, $a * e = a = e * a$, $\forall a \in G$

(iii) inverses: $\forall a \in G$, $\exists b \in G$ such that $a * b = e = b * a$

Definition 1.1.2
G is abelian if $a * b = b * a$ $\forall a, b \in G$.

Multiplicative notation: $ab = a * b$, $1 = e$, a^{-1} for the inverse of a
Additive notation: $ab = a + b$, $0 = e$, $-a$ for the inverse of a

Recall:

- The identity element e is unique
- The inverse of an element if unique
- $a_1a_2a_3 = (a_1a_2)a_3 = a_1(a_2a_3)$ (unambiguous)
- In general, $a_1a_2 \cdots a_n = (a_1 \cdots a_i)(a_{i+1} \cdots a_n)$
- $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$
- Cancellation laws: $ab = ac \implies b = c$, $ba = ca \implies b = c$

Application:
$a \in G$, $\varphi_a : G \to G$, $\varphi_a(x) = ax$
φ_a bijective if both injective and surjective.
Injective: $\varphi_a(x) = \varphi_a(y) \implies x = y$
Surjective: $\forall g \in G, \exists x$ such that $\varphi_a(g)$ with $x = a^{-1}g$

Definition 1.1.3
A homomorphism of groups is a map $f : G \to H$ such that

$$f(xy) = f(x)f(y) \quad \forall x, y \in G$$

An isomorphism is a bijective homomorphism.

Definition 1.1.4
Order of $G = |G|$ = cardinality of G.
For $a \in G$

$$\text{ord}(a) = \begin{cases} \min\{n \in \mathbb{Z}_+ \mid a^n = 1\} & \text{if such } n \text{ exists} \\ \infty & \text{if there exists no such } n \end{cases}$$

Notation:

$$a^n := \begin{cases} \overbrace{a \cdots a}^{n \text{ times}} & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

$a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Example 1.1.5 (Cyclic Groups)
$C_\infty = (\mathbb{Z}, +)$, $\quad C_n = (\mathbb{Z}/nZ, +)$
$\mathbb{Z}/n\mathbb{Z} = \{\widehat{0}, ..., \widehat{n-1}\}$
$\widehat{a} + \widehat{b} = \widehat{a+b}$
Exercise: $\text{ord}(\widehat{d}) = \frac{n}{(n,d)}$

Example 1.1.6 (Symmetric Groups)
A a set, then

$$S_A = \{f : A \to A \mid f \text{ bijective (“permutation of } A\text{”)}\}$$

with group operation $\alpha\beta = \alpha \circ \beta$ forms a group.
Symmetric group on n letters $S_n = S_{\{1,2,\ldots,n\}}$

m-cycles $(a_1 \ldots a_m)$ = permutation that sends a_1 to a_2, a_2 to a_3,$\ldots$ a_m to a_1 and leaves everything else. Such a cycle is said to have length m.
Exercise: $\text{ord}(m\text{-cycle}) = m$.

S_n is non-abelian for $m \geq 3$
e.g. $(12)(13) = (132)$, $(13)(12) = (123)$
$|S_n| = m!$, $S_2 = C_2$ and $S_1 = C_1$.

If $\alpha = \alpha_1\alpha_2 \cdots \alpha_k \in S_n$ product of disjoint cycles $\alpha_1, \ldots, \alpha_k$ of lengths $m_1, \ldots, m_k$, then $\text{ord}(\alpha) = \text{lcm}(m_1, \ldots, m_k)$.

$\alpha = (12)(568)(3479) \in S_n$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 7 & 6 & 8 & 9 & 5 & 3 & 10 \end{bmatrix} \qquad \text{ord}(\alpha) = 12$$

Remark: Disjoint cycles commute.

Theorem 1.1.7
$\forall \alpha \in S_n$, α is a product of disjoint cycles.

With above example, we have $\alpha = (3479)(12)(568)(\cancel{10})$.

Example 1.1.8 Matrices
Matrix groups over a field F, $(F = \mathbb{R}, \mathbb{C})$.

Definition 1.1.9
$M_n(F) = \{A | A = n \times n \text{ matrices with entries in } F\}$
$A = (a_{ij})$, $B = (b_{ij})$,

$$(A + B)_{ij} = (a_{ij} + b_{ij})$$

$M_n(F), +$ is a group.

$$(A \cdot B)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

$\cdot$ is associative, with identity, $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Definition 1.1.10
A is <u>invertible</u> if $\exists B$ such that $AB = BA = I$.

Theorem 1.1.11
A invertible $\iff \det A \neq 0$.

<u>General Linear Group</u>:
$GL_n(F) = \{A \in M_n(F) | A \text{ invertible}\}$
$(GL_n, \cdot)$ is a non-abelian group if $n \geq 2$.

$$A = \left[\begin{array}{c|c} U & 0 \\ \hline 0 & I \end{array}\right] \qquad B = \left[\begin{array}{c|c} V & 0 \\ \hline 0 & I \end{array}\right]$$

$AB \neq BA$ if $UV \neq VU$.

Example 1.1.12

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

<u>Orthogonal Group</u>:
$O_n(F) = \{A \in GL_n(F) \mid A^t A = I\}$
$(O_n, \cdot)$ is a group.
<u>Remark</u>:

(i) Condition on $A \implies (\det A)^2 = 1 \implies \det(A) = \pm 1$

(ii) Dot product of any column (row) of the matrix with itself equals 1

(iii) Dot product of any column (row) of the matrix with any other column (row) than itself equals 0

<u>Special Orthogonal Group</u>:
$SO_n(F) = \{A \in O_n(F) \mid \det A = 1\}$

<u>Summary</u>:

$$SO_n \subseteq O_n \subseteq GL_n$$

Example 1.1.13
$F = \mathbb{R}$

$SO_2 = \{A_\theta \mid \theta \in \mathbb{R}\}$

$$A_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \qquad \text{rotation by } \theta$$

$O_2 = \{A_\theta, B_\theta \mid \theta \in \mathbb{R}\}$

$$B_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \qquad \text{reflection about the line through origin in } \mathbb{R}^2$$

Lemma 1.1.14
Let S be a subset of a group G, $S \neq \emptyset$. If

(i) $\forall a, b \in S \implies ab \in S$

(ii) $\forall a \in S \implies a^{-1} \in S$

then S is a group (with binary operation on G).

Definition 1.1.15
A subset S as in lemma is called a subgroup of G, and we write $S \leq G$.
Remark: If G is finite, (i) $\implies$ (ii) in the lemma. Since if $S \subseteq G$:

$$\begin{aligned} \forall a \in S, \quad (\text{i}) &\implies a, a^2, a^3, \dots \text{ are in S} \\ &\implies a^n = a^m \text{ for some } n \neq m \\ &\implies \exists l > 0 \text{ integer such that } a^l = 1 \\ &\implies \forall a \in S, \operatorname{ord}(a) < \infty \\ &\implies (\text{ii}) \end{aligned}$$

Question: Does (i) $\implies$ (ii) if $|G| = \infty$? NO. $\mathbb{N} \not\leq \mathbb{Z}$.

Example 1.1.16
$SO_n \subseteq O_n \subseteq GL_n$.

1.2 Producing New Groups

(i) G, H groups

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

where the binary operation is defined by

$$(g, h)(g', h') = (gg', hh')$$

(ii) Centre of G

$$Z(G) = \{x \in G \mid xy = yx \quad \forall y \in G\}$$

Note that G abelian $\iff Z(G) = G$
Exercise: $Z(S_n) = \{\text{Id}\}$ if $n \geq 3$

(iii) Intersections of subgroups in a group G is a subgroup of G

(iv) If $f : G \to H$ homomorphism of groups

$$\ker f = \{x \in G \mid f(x) = 1\} \leq G$$
$$\operatorname{Im} f = \{f(x) \mid x \in G\} \leq H$$

Lemma 1.2.1
For any subset A of a group G, $\exists$ smallest subgroup H of G that contains A. Moreover, H = set of all products of elements of A and their inverses. (repetitions allowed)

Proof

$$H = \bigcap_{\substack{G' \leq G \\ G' \supseteq A}} G' \qquad \text{group using (iii).}$$

$H \supseteq A$
Let $H' :=$ set of products of elements in A and their inverses.

Claim: H' is a group

Proof of Claim:
$H' \supseteq A'$. $H \subseteq G \quad \forall G' \leq G, G' \supseteq A$.

□

Definition 1.2.2
A subset in G. $\langle A \rangle =$ smallest subgroup of G containing A = subgroup generated by A.
Remark: $a \in G$, $|\langle a \rangle| = \text{ord}(a)$.

Definition 1.2.3
A group G is cyclic if it is generated by one element, i.e. $\exists x \in G$ such that $G = \langle x \rangle$.
Remark: $G \cong \{A_{\frac{2\pi i}{n}} \mid i = 0, 1, \ldots, n-1\} \leq SO_2$
Exercise: For $n \geq 3$ C_n is isomorphic to the rotational group of symmetries of the regular n-gon. (rotations that preserve n-gon)

Recall: If $\text{ord}(x) = \infty$, $G = \langle x \rangle = \{x, x^{-1}, x^2, x^{-2}, \ldots\} \cong C_\infty$

Dihedral Groups:
D_{2n} = group of symmetries of the regular n-gon.

ζ = rotation by $\frac{2\pi}{n}$
s = reflection

$D_{2n} = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}, s, s\zeta, \ldots, s\zeta^{n-1}\}$. $\text{ord}(s) = 2$, $\text{ord}(\zeta) = n$, $\zeta s = s\zeta^{-1}$.

$$Z(D_{2n}) = \begin{cases} \{1\}, & n \text{ odd} \\ \{1, \zeta^{\frac{2}{n}}\}, & n \text{ even} \end{cases}$$

"D_4" $= V$ (Klein Four Group). $V \cong C_2 \times C_2$.
Exercise: $D_6 \cong S_3$ (smallest non-abelian group).

1.3 Facts on Groups of Symmetries

Definition 1.3.1
A function $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry if it preserves distance. i.e. $\forall v, w$, $||f(v) - f(w)|| = ||v - w||$.

Definition 1.3.2
If $F \subseteq \mathbb{R}^n$, the group of symmetries of F is the set of isometries that preserve F.

Theorem 1.3.3
Let $f : \mathbb{R}^n \to \mathbb{R}^n$, TFAE:

(i) f is an isometry and $f(0) = 0$

(ii) f preserves dot product, i.e. $f(v) \cdot f(w) = v \cdot w$

(iii) $f(x) = Ax$, $\forall x \in \mathbb{R}^n$, where $A \in O_n(\mathbb{R})$

Quaternion Group:
$Q = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = -1, ik = kj = -ji\}$.

1.4 Groups of Small Order

$\lvert G\rvert$	G	$\lvert G\rvert$	G
1	C_1	9	$C_9, C_3 \times C_3$
2	C_2	10	C_{10}, D_{10}
3	C_3	11	C_{11}
4	C_4, D_4	12	5 groups
5	C_5	13	C_{13}
6	C_6, D_6	14	C_{14}, D_{14}
7	C_7	15	C_{15}
8	$C_8, Q, D_8, C_2 \times C_4, C_2 \times C_2 \times C_2$		

Some Rules:

(i) $|G| = p$ (p prime) $\implies G \cong C_p$

(ii) $|G| = 2p$ (p prime) $\implies G \cong C_{2p}$ or D_{2p}

(iii) $|G| = p^2$ (p prime) $\implies G \cong C_{p^2}$ or $G \cong C_p \times C_p$

Example 1.4.1 (Homomorphisms)

(i) F a field, $GL_1(F) = F^\times (= F \setminus \{0\})$
Determinant map:

$$\det : GL_n(F) \to F^\times$$
$$\det(AB) = \det(A)\det(B)$$

(ii) (Cayley's Theorem:) $\exists$ injective homomorphism

$$\alpha : G \to S_G$$
$$\alpha(a) = \varphi_a$$
$$\varphi_a : G \to G$$
$$\varphi_a(x) = ax \quad \forall x \in G$$

Last time: $\varphi_a \in S_G$,
α is a homomorphism:

$$\alpha(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \alpha(a) \circ \alpha(b) \quad \forall a, b, \in G$$

α is injective:
Let $a \in G$ such that $\alpha(a) = Id \in S_G$,
$\implies \varphi_a = Id \implies \varphi_a(x) = Id(x) \quad \forall x \implies ax = x \quad \forall x \implies a = 1.$

Corollary 1.4.2
If $|G| = n$, $G = \{a_1, \ldots, a_n\}$, then $G \leq S_n$.

Multiplication table of G

$\cdot$	a_1	a_2	$\cdots$	a_n
a_1	a_1^2	a_1a_2	$\cdots$	a_1a_n
a_2	a_2a_1	a_2^2	$\cdots$	a_2a_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_na_1	a_na_2	$\cdots$	a_n^2

Any row is a permutation of $a_1, \ldots, a_n$.
$\alpha(a_i)$ = permutation given by i-th row.

$$\begin{bmatrix} a_1 \ldots a_n \\ -i\text{th row}- \end{bmatrix}$$

Properties of homomorphisms:

(i) $f(a^n) = f(a)^n \quad \forall a \in G, \quad \forall n$

(ii) $f(a^{-1}) = f(a)^{-1}$

1.5 Cosets

G a group, $S \subseteq G$ subset

$$aS = \{ax \mid x \in S\}$$
$$Sa = \{xa \mid x \in S\}$$

Remark: $abS = a(bS) = (ab)S$

Definition 1.5.1
$H \leq G$.

$aH =$ left coset of H in G
$Ha =$ right coset of H in G

Proposition 1.5.2
Let $H \leq G$. Then:

(i) $a \in G$ belongs to $bH \iff aH = bH$

(ii) $a, b \in G \implies$ either $aH = bH$ or $(aH) \cap (bH) = \emptyset$ (so left cosets form a partition of G)

(iii) $aH = bH \iff a^{-1}b \in H$

(iv) Any 2 left cosets of H in G have the same cardinality (possibly ∞)
In particular, $|aH| = |H| \quad \forall a \in G$

Remark: Same for right cosets, except in (iii). $Ha = Hb \implies ab^{-1} \in H$

Definition 1.5.3
The index $|G : H|$ of H in G is the number of left cosets of H in G.
Remark: # left cosets = # right cosets, $\exists$ bijection

$$\{aH \mid a \in G\} \to \{Hb \mid b \in G\}$$

surjective:

$$aH \mapsto Ha^{-1}$$
$$b^{-1}H \mapsto Hb$$

injective:

$$Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$$
$$\iff aH = bH$$

Example 1.5.4
$|G : 1| = |G|$, $|G : G| = 1$

Theorem 1.5.5 (Lagrange)
Let G be a finite group. Let $H \leq G$. Then

$$|G : H| = \frac{|G|}{|H|}$$

In particular, $|H| \Big| |G|$.

Proof
Let $k = |G : H|$. G finite $\implies k < \infty$ Consider the k distinct cosets.

$$a_1H, a_2H, \ldots, a_kH$$

These cosets form a partition of G

$$\implies |G| = \sum_{i=1}^{k} |a_iH| = k|H|$$

□

Corollary 1.5.6
G a finite group, then the order of any element divides $|G|$.

Corollary 1.5.7
For any prime p, if $|G| = p$, then $G \cong C_p$.
Remark: $\nexists$"converse" to Lagrange's theorem i.e. if $d \Big| |G|$ then generally $\nexists$ $H \leq G$ such that $|H| = d$.

Example 1.5.8
$A_4 = \{\text{all 3-cycles in } S_4\} \cup \{(12)(34), (13)(24), (14)(23)\}$ has no subgroup of order 6.

Part of Sylow's Theorem
$|G| = p^n k, (k, p) = 1$ (p prime) $\implies \exists H \leq G$ such that $|H| = p^n$.
Exercise: If either

(i) G is a p-group ($|G| = p^n, n$ integer > 0)

(ii) or G finite abelian group

then for all $d \mid G$, $\exists H \leq G$, $|H| = d$.

1.6 Normal Subgroups

$S, T \subseteq G$ subsets,

$$ST = \{xy \mid x \in S, y \in T\}$$

If $R, S, T \subseteq G$ subsets then $RT = (RS)T = R(ST)$.

Definition 1.6.1
A subgroup N of G is normal if $\forall x \in G$, $xNx^{-1} = N$, and we write $N \lhd G$.

Remark: $N \lhd G \iff xNx^{-1} \subseteq N \quad \forall x \in G$.

Proof

$$\begin{aligned} xNx^{-1} \subseteq N \quad \forall x &\iff y^{-1}Ny \quad \forall y \in G \\ &\iff N \subseteq yNy^{-1} \quad \forall y \in G \\ &\iff xNx^{-1} = N \quad \forall x \in G \end{aligned}$$

□

Proposition 1.6.2
$N \lhd G \iff xN = Nx \quad \forall x \in G$.

Proof
$xN = Nx \iff xNx^{-1} = N$. □

Remark: $xN = Nx$ means $\{xn \mid n \in N\} = \{n'x \mid n' \in N\}$.
In general, $xn \neq nx$, but $\forall n \in N$, $\exists n' \in N$ such that $xn = n'x$. Similarly for $(nx = xn')$.

Example 1.6.3

- $\{1\} \lhd G$, $G \lhd G$
- $Z(G) \lhd G$
- Any subgroup of index 2 is normal

  Proof
  Let $H \leq G$, $|G : H| = 2$. Then $\exists$ exactly 2 distinct left cosets: H, xH, for any $x \notin H$.

  $$\begin{aligned} &\implies G = H \sqcup xH \quad \text{(disjoint union)} \\ &\implies xH = G \setminus H \end{aligned}$$

  Similarly $Hx = G \setminus H$. Then $xH = Hx \; \forall x \in G$

  $$\implies xHx^{-1}H \forall x \notin H \implies H \lhd G$$

  □

- $D_{2n} = \{1, r \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\} \quad r^i s = sr^{-i}$
  $H = \langle r \rangle \cong C_n \implies |D_{2n} : H| = 2 \implies H \lhd D_{2n}$
  $r^{-1}s = sr^i \neq r^i s$ if $i \neq \frac{n}{2} sr^{-2i}$
  $\langle s \rangle = \{1, s\} \lhd D_{2n}$
  $r^i s r^{-i} \notin \{1, s\}$ (if $i \neq \frac{n}{2}$).
- Any subgroup of an abelian group is normal
- All subgroups of $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ are normal:

$$\left.\begin{array}{l} \{\pm 1, \pm i\} = \langle i \rangle \\ \langle j \rangle, \langle k \rangle \end{array}\right\} \text{ index 2}$$

$x(-1)x^{-1} \in \{\pm 1\} \quad \forall x \ \{\pm 1\} : i(-1)(-i) = i \cdot i = -1.$

Definition 1.6.4
A group G is simple if it contains no proper non-trivial normal subgroups.

Example 1.6.5

(i) C_p (p prime) is simple (Lagrange)

(ii) G abelian finite simple group $\implies G \cong C_p$.
(Homework)

$$d \big| |G| \implies \exists H \leq G, |H| = d \qquad (H \lhd G \text{ since } G \text{ abelian})$$

(iii) Smallest non-abelian simple group is A_5 (order 60)

Remark: Simple groups can still have lots of subgroups.

$$\textbf{Sylow's Theorem} : |G| = p^n k \qquad (k, p) = 1, p \text{ prime} \implies \exists \leq G, |H| = p^n$$

Homework $\implies H$ has subgroups of order p, p^2, $\ldots$, p^n
$\implies \forall$ finite group has non-trivial subgroups, unless it's C_p.

Proposition 1.6.6
If $H, N \leq G$, $N \lhd G$ then $HN \leq G$.
If $H, N \lhd G$ then $HN \lhd G$.

Example 1.6.7
$G = S_3$, $H = \langle (12) \rangle$, $N = \langle (13) \rangle$. $HN = \{Id, (12), (13), (12)(13)\} \not\leq S_3$.

Proof
Let hn, $h'n' \in HN$

$$(hn)(h'n') = h(nh')n' = h(h'm'')n' = \underbrace{hh'}_{\in H} \underbrace{m''n'}_{\in N} \implies (hn)(h'n') \in HN$$

$$xHNx^{-1} = \underbrace{xHx^{-1}}_{H} \underbrace{xNx^{-1}}_{N} = HN \quad \forall x \in G$$

□

Example 1.6.8
$G = D_{2n}$, $N = \langle r \rangle$, $H = \langle s \rangle$. $HN = G$.

Remark:

- $HN \leq G \iff HN = NH$
- Intersections of normal subgroups are normal subgroups

Proof
$x(H_1 \cap \cdots \cap H_k)x^{-1} \subseteq H_1 \cap \cdots \cap H_k, \quad \forall x \in G$ if $H_1, \ldots, H_k \lhd G$ □

Recall:
G a group, $A \subseteq G$ subset.

$$\langle A \rangle = \bigcap_{\substack{G' \leq G \\ A \subseteq G'}} = \{\text{products of } A \text{ and their inverses}\}$$

Lemma 1.6.9
$\langle A \rangle$ is normal $\iff xAx^{-1} \subseteq A \quad \forall x \in G$.

Proof
($\Rightarrow$) Clear.
($\Leftarrow$) The map "conjugation by x" is a homomorphism. Let $x \in G$. Let

$$\psi_x : G \to G$$
$$\psi_x(g) = xgx^{-1} \quad \forall g \in G$$

$\psi_x(g_1g_2) = \psi_x(g_1)\psi_x(g_2) \quad \forall g_1, g_2$.
$\langle A \rangle = \{a_1a_2 \cdots a_n \mid a_i \in A \text{ or } a_i^{-1} \in A \quad \forall i\}$

$$\langle A \rangle \lhd G \iff \psi_x(g) \in \langle A \rangle \quad \forall g \in \langle A \rangle$$

Let $g = a_1 \cdots a_n \in \langle A \rangle$,

$$\psi_x(g) = \psi_x(a_1) \cdots \psi_x(a_n)$$

If $a \in A$, $\psi_x(a) \in A$ by assumption. If $a^{-1} \in A$, $\psi_x(a) = \psi_x(a^{-1})^{-1}$, $\psi_x(a^{-1}) \in A$ □

Example 1.6.10
$G = D_{2n}$, $k \big| n$

$$\langle s^k \rangle \lhd G$$

Let t be a reflection. Check $tr^kt^{-1} \in \langle r^k \rangle$,

$$tr^kt^{-1} = tr^kt = r^{-k}tt = r^{-k} = r^{n-k} = r^{k(\frac{n}{k}-1)}$$

Proposition 1.6.11
The kernel of a homomorphism is a normal subgroup.

Proof
Let $f : G \to G'$ group hom.

$$\ker f = \{y \in G \mid f(y) = 1\}$$

Let $x \in G$. Let $y \in \ker f$. Then $f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = 1$. □

Example 1.6.12 (Special Linear Group)
$\det : GL_n(F) \to F^\times$

$$SL_n(F) := \ker(\det) = \{A \in M_n(F) \mid \det(A) = 1\}$$

is the special linear group.

$$SL_n(F) \lhd GL_n(F)$$

$A, B \in GL_n, A(SL_n) = B(SL_n) \iff \det A = \det B$

Proposition 1.6.13
Every normal subgroup occurs as the kernel of a homomorphism. If $H \lhd G$, then $\exists!$ group structure on the set G/H of cosets of H in G such that the map

$$\pi : G \to G/H$$
$$\pi(x) = xH$$

is a group homomorphism.

Proof
$G/H = \{xH \mid x \in G\}$. Define $(xH) \cdot (yH) = xyH$, $\forall x, y \in G$.
Need to prove:

(i) This is well defined

(ii) This gives a group structure on G/H

(iii) π is a hom

(iv) uniqueness

(iii) and (iv) are clear:

$$\begin{aligned} & \pi(xy) = \pi(x)\pi(y) \quad \forall x, y \\ \implies & xyH = (xH)(yH) \quad \forall x, y \end{aligned}$$

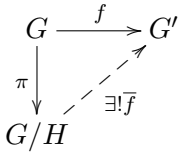
(i) Want to show that if $xH = x'H$, $yH = y'H$ then $xyH = x'y'H$. Equivalently, if $m = (xy)^{-1}x'y'$, then $m \in H$:

$$mH = (xy)^{-1}(x'y')H = y^{-1}x^{-1}H(x'y') = y^{-1}(x^{-1}Hx')y' = H$$

□

Universal Property of the Quotient map $\pi : G \to G/H$

$\forall f : G \to G'$ group homomorphism such that $f(H) = \{1\}$, then $\exists!$ $\overline{f} : G/H \to G'$ such that the diagram



commutes, $\overline{f} \circ \pi = f$.
Define $\overline{f} : G/H \to G'$, $\overline{f}(xH) = f(x)$. ($\overline{f}$ unique such that $\overline{f} \circ \pi = f$)

$\overline{f}$ is well-defined:
If $\underbrace{xH = yH}_{x^{-1}y \in H}$ then $f(x) = f(y)$,
$f(x^{-1}y) = 1$ since $f(H) = \{1\}$ then $f(x)^{-1}f(y) = 1 \implies f(x) = f(y)$

$\overline{f}$ is a homomorphism:
$\overline{f}((xH)(yH)) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH)$ □

Example 1.6.14 (Quotient Groups)

(i) $C_n = \mathbb{Z}/n\mathbb{Z}$

(ii) A_4 has unique non-trivial subgroup

$$H = \{Id, (12)(34), (13)(24), (14)(23)\}$$

$A_4/H \cong C_3$.

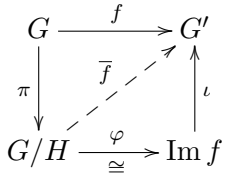
(iii) $k \big| n$, $\langle r^k \rangle \lhd D_{2n}$

Exercise: $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

$$\{\text{Subgroups of } G/H\} \longleftrightarrow \{\text{Subgroups of } G \text{ that contains } H\}$$
$$K/H \longleftarrow H \subseteq K \subseteq G$$
$$\overline{K} \subseteq G/H \longmapsto \pi^{-1}(\overline{K})$$

1.7 Isomorphism Theorems

Theorem 1.7.1 (First Isomorphism Theorem)
For any group homomorphism $f : G \to G'$, $H := \ker f$ is a normal subgroup of G, $\mathrm{Im}(f)$ is a subgroup of G' and f factors into the composite of a surjection, an isomorphism and an injective map.



Proof
$H \lhd G$, proved last time.
$\mathrm{Im}\, f \leq G'$ clear!
Universal property of quotients.

$$\implies \qquad \exists \overline{f} : G/H \to G' \text{ group homomorphism such that } f = \overline{f} \circ \pi$$

Define:

$$\varphi : G/H \to \mathrm{Im}(f) = \mathrm{Im}(\overline{f})$$
$$\varphi(xH) = f(x) \quad \forall x \in G$$

Claim: φ is an isomorphism

Proof of Claim:
φ is a homomorphism. Surjectivity is clear.

$$G_1 \xrightarrow{h \text{ gp hom.}} G_2 \implies G_1 \to h(G_2) \text{ also a group homomorphism and is surjective}$$

φ - injective

$$\begin{aligned} \ker \varphi &= \{xH \mid f(x) = 1\} \\ &= \{xH \mid x \in \ker f = H\} \\ &= \{H\} \qquad \blacksquare \end{aligned}$$

□

Corollary 1.7.2
If $f : G \to G'$ is a surjective group homomorphism then $G/\ker f \cong G'$.

Example 1.7.3
$C := \{z \in \mathbb{C} \mid |z| = 1\}$, $(C, \cdot)$ is an abelian group.
Remark:

$$\begin{aligned} (C, \cdot) &\cong SO_2 \\ e^{i\theta} &\mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = A_\theta \end{aligned}$$

Question: Is SO_n abelian for $n \geq 3$?
NO

$$\left(\begin{array}{c|c} A_\theta & 0 \\ \hline 0 & I \end{array}\right)\left(\begin{array}{c|c} B_\varphi & 0 \\ \hline 0 & -I \end{array}\right)$$

$(\mathbb{R}, +) \to \mathbb{R} \xrightarrow{f} C$, $f(x) = e^{2\pi i x}$

First isomorphism theorem $\implies \mathbb{R}/\mathbb{Z} \cong C$.

Example 1.7.4
$(\mathbb{C}^\times, \cdot) \xrightarrow{f} C$ by $f(z) = \frac{z}{|z|}$, then

$$\mathbb{C}^\times / \mathbb{R}_+ \cong C$$

Example 1.7.5
$C/\{\pm 1\} \cong C \qquad (z \mapsto z^2)$

Example 1.7.6
$GL_n(F)/SL_n(F) \cong F^\times$ by $\det : GL_n(F) \to F^\times$
$O_n(F)/SO_n(F) \cong C_2$ by $\det : O_n(F) \to F^\times$

Theorem 1.7.7 (Second Isomorphism Theorem)
Let $H \leq G$, $N \lhd G$. Then

(i) $HN \leq G$

(ii) $H \cap N \lhd H$

(iii) The map

$$H/(H \cap N) \xrightarrow{f} HN/N$$
$$f(x(H \cap N)) = xN$$

is an isomorphism.

Remark:

- If $H \cap N = \{1\}$, then $H \cong HN/N$ and $|HN| = |H||N|$
- If $|G| < \infty$, then $|H|/|H \cap N| = |HN|/|N|$
- If $|G| = |H||N|$, then $G = HN$ (and $H \cap N = \{1\}$)

Proof

(i) Last time

(ii) Prove that $\forall x \in H$, $x(H \cap N)x^{-1} \subseteq H \cap N$.
  (a) $x \in H \implies x(H \cap N)x^{-1} \subseteq H \cap N$
  (b) $N \lhd G \implies xNx^{-1} \subseteq N$

(iii) Let F be the composition of the quotient map $HN \to HN/N$. ($N \lhd G$ and $N \subseteq K \leq G \implies N \lhd K$)

$$\implies F(x) = xN \in HN/N$$

First isomorphism theorem $\implies$

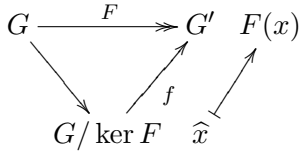
$$H/\ker F \cong HN/N$$

Prove that $\ker F = H \cap N$ and F is surjective:

$$\begin{aligned} \ker F &= \{x \in H \mid xN = N\} \\ &= \{x \in H \mid x \in N\} \\ &= H \cap N \end{aligned}$$

Let $yN \in HN/N$.
Prove $\exists x \in H$ such that $yN = xN$.
Let $x := h$. Then $hN = hmN$. ($N = mN$)

F induces f,



□

Remark: To have $H/(H \cap N) \cong HN/N$, it is enough to require $H \leq$ normaliser of N.

Definition 1.7.8
$A \subseteq G$ a set. the normaliser of A in G is

$$N_G(A) = \{x \in G \mid xAx^{-1} = A\}$$

Properties:

(i) $N_G(A) \leq G$

(ii) If $H \leq G$, $H \subseteq N_G(H) \subseteq G$

(iii) $H \lhd G \iff N_G(H) = G$

(iv) $H \lhd N_G(H)$

Exercise: $G = S_3$, $H = \langle (12) \rangle$ then $H \not\lhd G$.

Theorem 1.7.9 (Third Isomorphism Theorem)
Let $f : G \to G'$ be a surjective homomorphism of groups. Let $H := \ker f$. Then there exists a one-to-one correspondence as follows

$$\{\text{Subgroups of } G \text{ that contain } H\} \overset{1-1}{\longleftrightarrow} \{\text{Subgroups of } G'\}$$
$$H \subseteq K \longmapsto f(K)$$
$$f^{-1}(\overline{K}) \longmapsto \overline{K} \leq G'$$

Moreover, if $K \leftrightarrow \overline{K_1}$, $K_2 \longleftrightarrow \overline{K_2}$, then

(i) $\overline{K_1} \leq \overline{K_2} \iff K_1 \leq K_2$

(ii) $K \lhd G \iff \overline{K} \lhd G'$

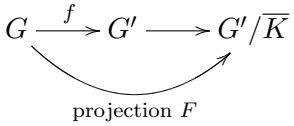
(iii) f induces an isomorphism

$$G/K \xrightarrow{\overline{f}} G'/\overline{K}$$
$$\overline{f}(xK) = f(x)\overline{K}$$

Proof

(i)-(ii) Exercise

(iii)



$$\ker F = \{x \in G \mid f(x) \in \overline{K}\}, \qquad F(x) = f(x)\overline{K}$$

□

1.8 Direct Products

$H_1, \ldots, H_k$ groups.

$$H_1 \times H_2 \times \ldots \times H_k = \{(h_1, h_2, \ldots, h_k) \mid h_i \in H_i\}$$

This is a group. The (external) direct product.

Definition 1.8.1
$H_1, \ldots, H_k \leq G$. G is the (internal) direct product of the subgroups $H_1, \ldots, H_k$ if the map

$$H_1 \times \ldots \times H_k \xrightarrow{\varphi} G$$
$$\varphi(h_1, \ldots, h_k) = h_1 h_2 \cdots h_k$$

is an isomorphism. i.e.

(i) $\forall x \in G$, $\exists!$ $h_i \in H_i$ in for each i such that $x = h_1 \cdots h_k$

(ii) If $x = h_1 \cdots h_k$, $y = h_1' \cdots h_k'$ then $xy = (h_1 h_1')(h_2 h_2') \cdots (h_k h_k')$

Proposition 1.8.2
A group G is an internal direct product of subgroups H_1, H_2 if

(i) $G = H_1 H_2$

(ii) $H_1 \cap H_2 = \{1\}$

(iii) $H_1 \lhd G$, $H_2 \lhd G$

or equivalently, (i),(ii) and (iii$'$) $xy = yx$ $\forall x \in H_1, y \in H_2$.

Proof
Assume G is an internal direct product of H_1, H_2:

(i) Obvious: $\exists \varphi : H_1 \times H_2 \to G$, $\varphi(h_1, h_2) \to = h_1 h_2$ isomorphism.

(ii) Let $x \in H_1 \cap H_2$, $x = x \cdot 1 = 1 \cdot x$, $\varphi(x, 1) = \varphi(1, x) \implies x = 1$

(iii) $\varphi(H_1 \times \{1\}) = H_1$, $\varphi(\{1\} \times H_2) = H_2$.
Fact exercise: $K_1 \lhd G_2, K_2 \lhd G_2 \implies K_1 \times K_2 \lhd G_1 \times G_2$
$\implies \{1\} \times H_2 \lhd H_1 \times H_2$, $H_1 \times \{1\} \lhd H_1 \times H_2$, and hence $H_1 \lhd G$, $H_2 \lhd G$.

(i),(ii), (iii) $\implies$ (iii$'$):

Let $x \in H_1$, $y \in H_2$. Show that $xyx^{-1}y^{-1} = 1$.
Enough to show $xyx^{-1}y^{-1} \in H_1 \cap H_2$:

$$xyx^{-1} \in H_2 \text{ since } H_2 \lhd G$$
$$yx^{-1}y^{-1} \in H_1 \text{ since } H_1 \lhd G$$

$\implies xyx^{-1}y^{-1} \in H_1 \cap H_2$.

(i),(ii),(iii$'$) $\implies$ direct product:

Let $\varphi : H_1 \times H_2 \to G$ by $\varphi(h_1, h_2) = h_1 h_2$

- Homomorphism clear by (iii$'$)
- Surjectivity follows from (i)
- Injective: $\ker \varphi = \{(h_1, h_2) \mid h_1 h_2 = 1\} = \{(1, 1)\}$ by (ii)

□

Remark: If G is an internal direct product of H_1, H_2, then

$$G/H_1 \cong H_2, G/H_2 \cong H_1$$

Proof
Second isomorphism theorem $\implies H_1 H_2/H_2 \cong H_1/H_1 \cap H_2$
G internal direct product $\implies G = H_1 H_2, H_1 \cap H_2 = \{1\}$ so $G/H_2 \cong H_1$ □

Difficulty:

$$\varphi : H_1 \times H_2 \longrightarrow G$$
$$\varphi(h_1, h_2) = h_1 h_2$$

$\varphi^{-1}(H_1) = H_1 \times \{1\}$ so $G/H_1 \cong H_2$ is the same as $H_1 \times H_2/H_1 \times \{1\} \cong H_2$.

Lemma 1.8.3
$C_{mn} \cong C_m \times C_n \iff (m,n) = 1.$

Proof
If $(m,n) = 1$, $G = C_{mn} = \mathbb{Z}/mn\mathbb{Z}$, $H_1 = \langle \widehat{m} \rangle$, $H_2 = \langle \widehat{n} \rangle$

$$\begin{aligned} \operatorname{ord}(\widehat{m}) &= n, \quad H_1 \cong C_n \\ \operatorname{ord}(\widehat{n}) &= m, \quad H_2 \cong C_m \end{aligned}$$

Check (i),(ii),(iii):

(ii) $|H_1 \cap H_2| \Big| m, n$ by Lagrange's Theorem. $(m,n) = 1 \implies |H_1 \cap H_2| = 1$

(i) Second isomorphism theorem $\implies H_1H_2/H_1 \cong H_2/H_1 \cap H_2$

$$H_1 \cap H_2 = \{1\} \implies |H_1H_2| = |H_1||H_2| = mn = |G| \implies G = H_1H_2$$

(iii′) Clear since G abelian

So $G \cong H_1 \times H_2$.

If $(m,n) \neq 1$, then $C_m \ncong C_m \times C_n$ and so $\nexists x \in C_m \times C_n$ such that $\operatorname{ord}(x) = mn$. If $l = \operatorname{lcm}(m,n)$ then $\operatorname{ord}(x) \leq l \quad \forall x \in C_m \times C_n$. Since $(m,n) \neq 1$, $l < mn$. □

Example 1.8.4
If n odd, then $D_{4n} \cong D_{2n} \times C_2$
If n even, then $D_{4n} \ncong D_{2n} \times C_2$

<u>1st case</u>: $D_{12} \cong D_6 \times C_2$ $(\cong S_3 \times C_2)$

Assume <u>n odd</u>:

$G := D_{4n} = \{1, r, r^2, \ldots, r^{2n-1}, s, sr, \ldots, sr^{2n-1}\}$

$$\begin{aligned} H_1 &= \langle r^n \rangle = \{1, r^n\} \\ H_2 &= \langle r^2, s \rangle = \{1, r^2, r^4, \ldots, r^{2n-2}, s, sr^2, sr^4, \ldots, s^{2n-2}\} \quad (2n \text{ elements}) \end{aligned}$$

Check (i)-(iii) in proposition:

(iii) $H_2 \lhd G$ since $|G : H_2| = 2$ and $H_1 = Z(D_{4n}) \lhd D_{4n}$. (Exercise: $\langle r^i \rangle \lhd D_{2n} \quad \forall i$)

(ii) $H_1 \cap H_2 = \{1\} : r^n \notin H_2$ because

$$\begin{aligned} r^n &\neq r^{2k} \quad \forall k \text{ since } n \text{ odd} \\ r^n &\neq sr^{2k} \quad \forall k \text{ since otherwise } s \in \langle r \rangle \end{aligned}$$

(i) $G = H_1H_2$: prove $|H_1H_2| = 4n$. Use second isomorphism theorem:

$$\begin{aligned} & H_1H_2/H_1 \cong H_2/H_1 \cap H_2 \\ \implies & |H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = |H_1||H_2| = 2(2n) = 4n \\ \implies & G = H_1H_2 \end{aligned}$$

<u>2nd Case</u>: Recall

$$Z(D_{2n}) = \begin{cases} \{1\} & \text{if } n \text{ odd} \\ \{1, r^{\frac{n}{2}}\} & \text{if } n \text{ even} \end{cases}$$

Exercise: $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$ (equality of subgroups in $G_1 \times G_2$).

Assume n even. If $D_{4n} \cong D_{2n} \times D_{2n}$, then

$$\underbrace{Z(D_{4n})}_{2 \text{ elements}} \cong Z(D_{2n} \times C_2) = \underbrace{\underbrace{Z(D_{2n})}_{2 \text{ elements}} \times \underbrace{Z(C_2)}_{2 \text{ elements}}}_{4 \text{ elements}}$$

Contradiction.

Example 1.8.5
$O_n \cong SO_n \times C_2$ if n odd
$O_n \ncong SO_n \times C_2$ if n even.

For example $O_2 \ncong SO_2 \times C_2$, since LHS is nonabelian, but RHS is abelian.

Proposition 1.8.6
G group, $H_1, \ldots, H_k \leq G$. Then G is an internal direct product of $H_1 \ldots H_k \iff$

(i) $G = H_1 H_2 \cdots H_k$

(ii) $\forall j, \quad H_j \cap H_i \cdots H_{j-1} H_{j+1} \cdots H_n = \{1\}$

(iii) $H_j \lhd G \quad \forall j$

and (i)-(iii) $\iff$ (i)-(iii′): $\forall i \neq j$, $\forall x \in H_i$, $\forall y \in H_j, xy = yx$

Proof
Assume G is an internal direct product of $H_1, \ldots, H_k$ then

$$\varphi : H_1 \times \cdots \times H_k \to G$$
$$\varphi(h_1, \ldots, h_k) = h_1 \cdots h_k$$

is an isomorphism, so

(i) $\mathrm{Im}(\varphi) = H_1 \cdots H_k \implies G = H_1 \cdots H_k$

(ii) Let

$$A_j := \{1\} \times \cdots \{1\} \times H_j \times \{1\} \times \cdots \{1\}$$

Then $\varphi(A_j) = H_j$

$$B_j := H_1 \times \cdots \times H_{j-1} \times \{1\} \times H_{j+1} \times \cdots H_k$$

Then $\varphi(B_j) = H_1 \cdots H_{j-1} H_{j+1} \cdots H_k$.
Since φ is an isomorphism,

$$H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k) = \{1\} \iff A_j \cap B_j = \{1\}$$

(iii) $H_j \lhd G \iff A_j \lhd (H_1 \times \cdots \times H_k)$

(i),(ii),(iii) $\implies$ (iii′) Let $x \in H_i$, $y \in H_j$. Then $xyx^{-1}y^{-1} = 1$ since:

$$H_j \lhd G \implies (xyx^{-1}) \in H_j \implies xyx^{-1}y^{-1} \in H_j$$
$$\text{Same argument} \implies xyx^{-1}y^{-1} \in H_i$$
$$\implies xyx^{-1}y^{-1} = 1$$

(i)(ii)(iii′) $\implies$

$$\varphi : H_1 \times \cdots \times H_k \to G$$
$$\varphi(h_1, \ldots, h_k) = h_1 \cdots h_k$$

is an isomorphism.

- φ is a homomorphism follows from (iii′)
- φ surjective follows from (i)
- φ injective:
  Let $h_i \in H_i$ such that $h_1 h_2 \cdots h_k = 1$ then $h_2 \cdots h_k = h_1^{-1} \in H_1 \cap (H_2 \cdots H_k) \implies h_1 = 1$. Same for all h_i using (iii′)

□

Remark:

(i) $H_1, H_2, \ldots, H_k \lhd G$ by induction, $k = 2$ proved.

(ii) If G is an internal direct product of $H_1, \ldots, H_k$ then G is internal direct product of $(H_1 \cdots H_i)(H_{i+1} \cdots H_k)$.

Classification of Groups of Order 8

$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$, D_8, Q.

$G \cong C_8 \iff \exists x \in G$ with $\text{ord}(x) = 8$.

Assume $\nexists x \in G$ with $\text{ord}(x) = 8$. Then any non-trivial $x \in G$ will have order 2 or 4.

Assume further that $\forall x \in G$, $\text{ord}(x) = 2$.

Claim: G is abelian.

Proof of Claim:
$(xy)^2 = 1 \quad \forall x, y \in G$
$\implies xyxy = 1 \implies xy = yx.$ ■

Let $x, y \in G$, $x, y \neq 1$.
Let $z \in G$, $z \neq 1, x, y, xy$
Let $H_1 = \langle x \rangle$, $H_2 = \langle y \rangle$, $H_3 = \langle z \rangle$.
Check (i),(ii),(iii′):

(iii) Clear. G abelian.

(ii)

$$H_1 \cap H_2 H_3 = \{1\} \iff x \notin \{1, y, z, yz\}$$
$$H_2 \cap H_1 H_3 = \{1\} \iff y \notin \{1, x, z, xz\}$$
$$H_3 \cap H_1 H_2 = \{1\} \iff z \notin \{1, x, y, xy\}$$

(i) By second isomorphism theorem:

$$|H_1 H_2 H_3| = |H_1||H_2 H_3|/|H_1 \cap H_2 H_3| = 8$$

$\implies G \cong H_1 \times H_2 \times H_3$, $C_2 \times C_2 \times C_2$

Assume $\exists x \in G$, $\text{ord}(x) = 4$.
Let $H = \langle\, x \,\rangle = \{1, x, x^2, x^3\}$, $H \lhd G$ since $|G : H| = 2$.
Also, $G = H \sqcup yH$ for all $y \notin H$. Pick $y \notin H$, then

$$G = H \sqcup yH = \{\underbrace{1, x, x^2, x^3}_{H}, \underbrace{y, yx, yx^2, y^3}_{yH=Hy}\}$$

$xy \in Hy \implies xy \notin H \implies xy \in \{y, yx, yx^2, yx^3\}$

Claim: $xy \neq yx^2$

Proof of Claim:
$x = yx^2y^{-1} \implies x^2 = (yx^2y^{-1})(yx^2y^{-1}) = 1$. Contradiction. ■

Claim: $y^2 \in H$

Proof of Claim:
In fact, $y^2 \in \{1, x^2\}$ since $\text{ord}(x) = \text{ord}(x^3) = 4$. ■

Four cases:

I. $xy = yx$, $y^2 = 1$
Let $K = \langle\, y \,\rangle$. Then $G \cong H \times K$. $H \cap K = \{1\}$. Elements of H commute with elements of K because $xy = yx$. So $|HK| = 8 \implies G = HK$, so $G \cong C_4 \times C_2$.

II. $xy = yx$, $y^2 = x^2$. Same proof gives $G \cong C_4 \times C_2$

III. $xy = yx^3 = yx^{-1}$, $y^2 = 1 \implies G = D_8$

IV. $xy = yx^3 = yx^{-1}$, $y^2 = x^2$

$$Q \cong G \qquad \begin{aligned} Q &\longrightarrow G \\ i &\longmapsto x \\ j &\longmapsto y \end{aligned}$$

Lemma 1.8.7
G abelian, $|G| = p_1 \cdots p_k$ (distinct primes), then $G \cong C_{p_1 \cdots p_k}$.

Proof
By Cauchy's Theorem, let $x_1, \ldots, x_k \in G$, $\text{ord}(x_i) = p_i$. Let $H_i = \langle\, x_i \,\rangle$.

Claim: G is an internal direct product of $H_1, \ldots, H_k$.

Proof of Claim:
$H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k) = \{1\}$
$|H_{i_1} \cdots H_{i_m}| = p_{i_1} \cdots p_{i_m} \quad \forall i_1, \ldots i_m$.

So by Lagrange, $|H_j \cap H_1 \ldots H_k|$ divides p_j and $p_1 \cdots p_{j-1} p_{j+1} \cdots p_k$. Also, $G = H_1 \cdots H_k$ follows from same fact. Above uses Lagrange's theorem and induction on m. ■

$\implies G \cong C_{p_1} \times \cdots \times C_{p_k} \cong C_{p_1 \cdots p_k}$ by coprimality. □

Corollary 1.8.8
G abelian, $|G| = mn$, $(m, n) = 1$, then $G \cong H \times K$, $\forall H, K \leq G$ where $|H| = m$, $|K| = n$.

1.9 Automorphisms

Definition 1.9.1
An automorphism of G is an isomorphism $G \xrightarrow{f} G$. We write

$$\mathrm{Aut}(G) = \{f \mid f : G \to G \text{ automorphism}\}$$

Exercise: $(\mathrm{Aut}(G), \circ)$ is a group.

For $g \in G$, consider the "conjugation by g"

$$\begin{aligned} \psi_g &: G \to G \\ \psi_g(x) &= gxg^{-1} \quad \forall x \in G \end{aligned}$$

Exercise: $\psi_g \in \mathrm{Aut}(G)$
Remark:

$$\psi_{gh}(x) = gh(x)(gh)^{-1} = ghxh^{-1}g^{-1} = \psi_g \circ \psi_h(x)$$

Let

$$\begin{aligned} u &: G \to \mathrm{Aut}(G) \\ u(g) &= \psi_g \end{aligned}$$

Remark $\implies$ u is a group homomorphism.

Definition 1.9.2

$$\mathrm{Inn}(G) := \mathrm{Im}(u) = \{\psi_g \mid g \in G\} \leq \mathrm{Aut}(G)$$

is the inner automorphisms.
Any $f \in \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$ is called an outer automorphism.
Remark: If G abelian then $\mathrm{Inn}(G) = \{Id_G\}$.

Lemma 1.9.3
The map $u : G \to \mathrm{Aut}(G)$ has kernel $Z(G)$.

Proof
$\ker u = \{g \in G \mid \psi_g = Id_G\} = Z(G)$. □

Corollary 1.9.4
$G/Z(G) \cong \mathrm{Inn}(G)$.
Remark: $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

If $f \in \mathrm{Aut}(G)$,

$$\begin{aligned} f \circ \psi_g \circ f^{-1}(x) &= f(gf^{-1}(x)g^{-1}) \\ &= f(g)xf(g)^{-1} \\ \implies f \circ \psi_g \circ f^{-1} &= \psi_{f(g)} \end{aligned}$$

Example 1.9.5
$G = \underbrace{C_p \times \cdots \times C_p}_{n \text{ times}} (= (\mathbb{F}_p^n, +))$ elementary abelian group of order p^n

Any homomorphism $f : G \to G'$ is determined by $f(e_i)$ where $e_i = (0, \ldots, 0, \underbrace{\widehat{1}}_{i^{th}}, 0, \ldots, 0)$. $\widehat{x} = \widehat{1}$.

Why:

$$f(\widehat{x_1}, \ldots, \widehat{x_n}) = x_1 f(e_1) + \ldots + x_n f(e_n)$$

$x_1, \ldots, x_n \in \{0, 1, \ldots, p-1\}$

$$\begin{aligned}(\widehat{x_1}, \ldots, \widehat{x_n}) &= (\widehat{x_1}, \widehat{0}, \ldots, \widehat{0}) + \cdots + (0, \ldots, \widehat{0}, \widehat{x_n}) \\ &= x_1 e_1 + \cdots + x_n e_n\end{aligned}$$

where $\widehat{x} = \underbrace{\widehat{1} + \cdots + \widehat{1}}_{x \text{ times}}$

$\forall f : G \to G$ is given by $f(\vec{x}) = A\vec{x}$, $A \in M_n(\mathbb{F}_p)$.

Let $\vec{a_i} = f(e_i) \in \mathbb{F}_p^n$. Let $A = [\vec{a_1}, \ldots, \vec{a_n}]$.

$$A\vec{x} = x_1\vec{a_1} + \ldots + x_n\vec{a_n}$$

$\mathrm{Aut}(G) \cong GL_n(\mathbb{F}_p)$.

If $\begin{matrix} f(\vec{x}) = A\vec{x} \\ g(\vec{x}) = B\vec{x} \end{matrix}$, then $f \circ g(x) = ABx$

Example 1.9.6 (Particular Case)
$G = C_2 \times C_2 (= V)$

$$\mathrm{Aut}(V) \cong GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Exercise: $\mathrm{Aut}(V) = S_3$.

Or, $V = \{1, x, y, xy\}$. Any permutation of $\{x, y, xy\}$ is an element in $\mathrm{Aut}(V)$.

Example 1.9.7
$Q =$ quaternion group

$\mathrm{Inn}(Q) \cong Q/Z(Q) \cong V, Z(Q) = \{\pm 1\}$
$\mathrm{Aut}(Q) \cong S_4$

$\forall f \in \mathrm{Aut}(Q), f(i), f(j), f(k) \in \{\pm i, \pm j, \pm k\}$
There are 4 choices for the map f.

Example 1.9.8
$G = S_n$ (Later: $Z(S_n) = \{Id\}$ for $n \neq 2$)
. Corollary $\implies \mathrm{Inn}(S_n) \cong S_n$
Exercise later:
If $n \neq 6$, then $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ $(\cong S_n)$
If $n = 6$, then $|\mathrm{Aut}(S_n) : \mathrm{Inn}(S_n)| = 2$

Special Case: $\mathrm{Aut}(S_3) = S_3$. $\forall f \in \mathrm{Aut}(S_3)$ permutes $(12), (13), (23)$.

1.10 Automorphisms of Cyclic Groups

Lemma 1.10.1
Let $G = C_n$. Then $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &= \{\widehat{k} \in \mathbb{Z}/n\mathbb{Z} \mid (k,n) = 1\} \\ &= \{\widehat{k} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \widehat{l} \in \mathbb{Z}/n\mathbb{Z}, \widehat{k} \cdot \widehat{l} = \widehat{1}\}\end{aligned}$$

Euler Totient Function: $\#\{k \in \mathbb{Z} \mid k > 0, k < n, (k,n) = 1\}$

Proof

Remark:

- $\forall f \in \mathrm{Aut}(G)$, f map generators of G to generators of G. Let $\widehat{a} = f(\widehat{1})$. Then $(a,n) = 1$.
- If $f(\widehat{1}) = \widehat{a}$ a homomorphism. $f : G \to G$, then $f(\widehat{m}) = \widehat{ma} = m\widehat{a} \quad \forall m \in \mathbb{Z}$.
  We write $f_{\widehat{a}} : G \to G$, $f_{\widehat{a}}(\widehat{m}) = \widehat{ma}$ $\forall m \in \mathbb{Z}$.
- $f_{\widehat{a}}$ is a group homomorphism, $f_{\widehat{a}} \circ f_{\widehat{b}} = f_{\widehat{ab}}$
- $f_{\widehat{a}} \in \mathrm{Aut}(G) \iff (a,n) = 1$, so $\widehat{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Define

$$\begin{aligned}u : (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(G) \\ \widehat{a} &\mapsto f_{\widehat{a}}\end{aligned}$$

u is an isomorphism of groups. u injective: $f_{\widehat{a}}(\widehat{1}) = \widehat{a}$. □

$C_n = \mathbb{Z}/n\mathbb{Z}$

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times, (f : C_n \to C_n) \mapsto f(\widehat{1}) \qquad (\widehat{1} = 1 \bmod n)$$

$C_\infty = \mathbb{Z}$

$$\mathrm{Aut}(C_\infty) \cong C_2 = \{Id_{\mathbb{Z}}, x \mapsto -x\}$$

Question: What is $(\mathbb{Z}/n\mathbb{Z})^\times$? Proved: $C_{mn} \cong C_m \times C_n \iff (m,n) = 1$

Theorem 1.10.2 (Chinese Remainder Theorem)
If (m,n)=1, then

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\xrightarrow{\phi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (k \bmod mn) &\mapsto (k \bmod m, k \bmod n)\end{aligned}$$

is an isomorphism of rings.

Proof
φ homomorphism: $\begin{array}{l}(k+l) \bmod m = k \bmod m + l \bmod m \\ (k \cdot l) \bmod m = (k \bmod m) \cdot (k \bmod n)\end{array}$.

φ well-defined: $k \bmod mn = 0$, (so $mn|k$) $\implies$ $\begin{array}{ll}k \bmod m = 0 & m|k \\ k \bmod n = 0 & n|k\end{array}$

φ injective: $\begin{matrix} k \bmod m = 0 & (m|k) \\ k \bmod n = 0 & (n|k) \end{matrix} \implies k \bmod mn = 0 \quad (mn|k)$

φ surjective: $(m,n) = 1 \implies \exists x, y \in \mathbb{Z}, xm + yn = 1$
Given $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \varphi(ayn + bxm) = (a,b)$
since $1 = (xm + yn) \equiv (yn) \bmod m$.

□

Corollary 1.10.3
If $(m,n) = 1$ then $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

Recall: $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$
$\implies \varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$

Corollary 1.10.4
If $n = p_1^{r_1} \cdots p_s^{r_s}$ (p_i distinct primes)

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times$$

Question: What is $(\mathbb{Z}/p^n\mathbb{Z})^\times$?

$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$

Proposition 1.10.5 (i) If p is an odd prime, then $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is a cyclic group, i.e. $(\mathbb{Z}/p^r\mathbb{Z})^\times \cong C_{p^{r-1}(p-1)}$

(ii) If $p = 2$ then $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong C_{r-2} \times C_2$

Theorem 1.10.6 (Structure Theorem for Finitely Generated Abelian Groups)
G finitely generated abelian group, then G is a product of cyclic groups.

Theorem 1.10.7
F field, $G \leq F^\times$ finite subgroup $\implies$ G cyclic.

Corollary 1.10.8
$\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Recall: G abelian group, $|G| = mn$, $(m,n) = 1$. Then $G \cong H_1 \times H_2$ for any $H_1, H_2 \leq G$, $|H_1| = m$, $|H_2| = n$

Proof of Proposition

(i) To show $G = (\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic, it is enough to find $H_1, H_2 \leq G$ cyclic $|H_1| = p^{r-1}$, $|H_2| = p-1$
Exercise: $\widehat{p+1} \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ is an element of order p^{r-1}.
Let $H_1 = \langle \widehat{p+1} \rangle \cong C_{p^{r-1}}$

Claim: Any subgroup of $G = (\mathbb{Z}/p^r\mathbb{Z})^\times$ of order $p-1$ is cyclic.
Proof of Claim:

Let $H \leq G$, $|H| = p-1$

$$\mathbb{Z}/p^r\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z}$$
$$\pi(k \bmod p^r) = (k \bmod p)$$

surjective ring hom.
Let

$$f : (\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$
$$k \bmod p^r \mapsto k \bmod p \quad \forall k = 1, p-1$$

be the induced map on units then f is a surjective group homomorphism.
First isomorphism theorem $\implies$:

$$|\ker(f)| = \frac{p^{r-1}(p-1)}{p-1} = p^{r-1}$$

Notice that since $|H| = p-1$, $|\ker(f)| = p^{r-1}$, $(p-1, p^{r-1}) = 1$.
So Lagrange $\implies$ $H \cap \ker(f) = \{1\}$.

$$H \underset{h}{\subseteq} (\mathbb{Z}/p^r\mathbb{Z})^\times \xrightarrow{f} (\mathbb{Z}/p\mathbb{Z})^\times$$

$h : H \to (\mathbb{Z}/p\mathbb{Z})^\times$ is an injectice homomorphism of groups.
Since $H \cap \ker(f) = 1 \implies h$ isomorphism of groups.
Theorem $\implies$ $H \cong \mathbb{F}_p^\times$ cyclic, $|H| = p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times$

Assuming the claim, pick any $H_2 \leq G$, $|H_2| = p-1$.

(ii)

Exercise:

(a) $\exists$ element of order 2^{r-2} in $(\mathbb{Z}/2^r)^\times$

(b) $(\mathbb{Z}/2^r\mathbb{Z})^\times$ not cyclic.

$$\implies \underbrace{(\mathbb{Z}/2^r\mathbb{Z})^\times}_{\text{order } 2^{r-1}} \cong \underbrace{C_{2^{r-2}}}_{C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}} \times C_2$$

□

1.11 Characteristic Subgroups

Definition 1.11.1
$H \leq G$ is called a characteristic subgroup if for all $f \in \mathrm{Aut}(G)$, $f(H) = H$.
Remark:

(i) Enough to show $f(H) \subseteq H \quad \forall f \in \mathrm{Aut}(G)$

(ii) $H \lhd G \iff f(H) \subseteq H \quad \forall f \in \mathrm{Inn}(G)$, ={aut by conjugation}

$\implies$ characteristic subgroups are normal.

Example 1.11.2

(i) $Z(G)$ is a characteristic subgroup of G:
If $x \in Z(G)$, then $f(x) \in Z(G)\ \forall f \in \mathrm{Aut}(G)$

$$f(x)f(y) = f(y)f(x)$$
$$f(xy) = f(xy)$$

since $x \in Z(G)$.

(ii) If $H \leq G$ is the unique subgroup of order m for some m, then H is a characteristic subgroup.
Exercise: $H = \{Id, (12)(34), (13)(24), (14)(23)\} \leq A_4$ unique subgroup of order 4 in A_4.
$\implies H \lhd A_4$.

(iii) G group. $[x, y] := xyx^{-1}y^{-1}$

$$[G, G] := \text{ subgroup of } G \text{ generated by all } [x, y], \forall x, y \in G$$

is called the commutator subgroup of G.
This is a characteristic subgroup of G: if $f \in \mathrm{Aut}(G)$, then $[f(x), f(y)] = f([x, y])$.

Remark:

- G abelian $\iff [G, G] = 1$
- If $H \lhd G$, then G/H abelian $\iff H \supseteq [G, G]$
- $N \lhd G$, $H \lhd G \not\Rightarrow H \lhd G$

Example 1.11.3
$G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, $N = \{1, r^2, s, sr^2\}$, $H = \{1, s\}$.

$H \lhd N$ (N abelian), $N \lhd G$, ([G:N]=2), but $H \not\lhd G$.

Lemma 1.11.4
If H is a characteristic subgroup of N, $N \lhd G$, then $H \lhd G$.

Example 1.11.5
$Z(N), [N, N] \lhd G$ (if $N \lhd G$).

Proof

$$\psi_g : G \to G$$
$$\psi_g(x) = gxg^{-1}$$

is in $\mathrm{Aut}(G)$.

$$N \lhd G \iff \psi_g(N) \subseteq N$$

$\underbrace{\psi_g|_N}_{\substack{\text{restricting} \\ \psi_g \text{ to } N}}$ $: N \to N$ is an automorphism of N, since $\psi_g(N) \supseteq N$. In fact $\psi_g(N) = N$.

$$\implies \psi_{g|_N}(H) \subseteq H \implies \psi_g(H) \subseteq H \iff H \lhd G$$

□

1.12 Semidirect Products

H, K groups. $\varphi : K \to \mathrm{Aut}(H)$ homomorphism of groups.

Definition 1.12.1
The semidirect product of groups H and K is

$$H \rtimes_\varphi K = \{(x, y) \mid x \in H, y \in K\}$$

where multiplication is defined by

$$(x, y)(x', y') = (x\varphi(y)(x'), yy')$$

If φ is the trivial homomorphism, we recover the normal direct product.
Even if H, K are abelian, $H \rtimes_\phi K$ might not be abelian

This is a group:

- Identity $(1_H, 1_K)$
- Associativity - straightforward
- $(x, y)^{-1} = (\varphi(y^{-1})(x^{-1}), y^{-1})$
  Check:

$$\begin{aligned}(x, y)(\varphi(y^{-1})(x^{-1}), y^{-1}) &= (x\varphi(y)\varphi(y^{-1})x^{-1}, yy^{-1}) \\ &= (x[\varphi(y) \circ \varphi(y^{-1})](x^{-1}), yy^{-1}) \\ &= (xx^{-1}, 1) \\ &= (1, 1)\end{aligned}$$

Properties $G := H \rtimes_\varphi K$

(i) $|H \rtimes K| = |H||K|$

(ii) H, K are isomorphic to subgroups of G via this identification

(iii) $H \lhd G$, $G/H \cong K$ (via $K \subseteq G \to G/H$)

(iv) $H \cap K = \{1\}$

(v) $G = HK$ as sets

(vi) TFAE

(a) $K \lhd G$

(b) $\varphi =$ trivial map

(c) $H \rtimes K \cong H \times K$ by $(h, k) \mapsto (h, k)$

Proof

(i) Clear.

(ii) H and K are isomorphic to $H' = \{(x, 1) \mid x \in H\} \subseteq G$
$K' = \{(1, y) \mid y \in K\} \subseteq G$ respectively by

$$x \mapsto (x, 1) \qquad \text{and} \qquad y \mapsto (1, y)$$

(iii) Let $f : G \to K$, $f(x,y) = y$. Then f is a homomorphism:

$$\begin{aligned} f((x,y)(x',y')) &= f(x\varphi(y)(x'), yy') \\ &= yy' \\ &= f(x,y)f(x',y') \end{aligned}$$

$\ker f = \{(x,1) \mid x \in H\} = H'$. And f is clearly surjective.
By isomorphism theorem, $G/\ker f = G/H \cong K$. Also:

$$\begin{array}{ccc} K \subseteq G & \longrightarrow & G/H \\ & \underset{g}{\curvearrowright} & \end{array}$$

$$y \mapsto (1,y) \mapsto \widehat{(1,y)} := \text{ coset of } (1,y)$$

g is a homomorphism of groups.

$$\ker(g) = \{y \in K \mid (1,y) \in H\} = \{(1,1)\}$$

g is surjective:
Let $(x,y) \in G$, show

$$\widehat{(x,y)} = \widehat{(1,y)} \qquad (\iff (x,y)^{-1}(1,y) \in H)$$

$$\begin{aligned} (\varphi(y^{-1})(x^{-1}), y^{-1}) &= (\varphi(y^{-1})(x^{-1})\varphi(y^{-1})(1), y^{-1}y) \\ &= (x,y)^{-1} \end{aligned}$$

$\implies$ g is an isomorphism.

(iv) $H' \cap K' = \{(1,1)\}$

(v) $(x,y) = (x,1)(1,y) = (x\varphi(1)(1), 1 \cdot y)$

(vi) (b) $\implies$ (c), clear
(c) $\implies$ (a)

$$K' = \{1\} \times K \subseteq H \times K \text{ normal subgroup}$$

$\implies K \lhd G$
(a) $\implies$ (b)

$$K \lhd G \iff \quad \forall x \in H$$

$(1,y') = (x,1)(1,y)(x,1)^{-1} \in K$ for some $y' \in K$.
$(x,1)^{-1} = (\varphi(1^{-1})(x^{-1}), 1^{-1}) = (x^{-1}, 1)$

$$\begin{aligned} & (x,1)(1,y)(x^{-1}) = (1,y') \\ \implies \quad & (x\varphi(x^{-1}), y) = (x,y)(x^{-1},1) = (1,y') \\ \implies \quad & x\varphi(y)(x^{-1}) = x^{-1} \qquad \forall x \in H, \forall y \in K \\ \implies \quad & \varphi(y)(x^{-1}) = x^{-1} \qquad \forall x \in H, \forall y \in K \\ \implies \quad & \varphi(y) = Id_H \qquad \forall y \in K \\ \implies \quad & \varphi = \text{ trivial} \end{aligned}$$

□

Proposition 1.12.2
Let H, K be subgroups of a group G. Assume that

(i) $G = HK$

(ii) $H \cap K = \{1\}$

(iii) $H \lhd G$

Then $G \cong H \rtimes_\varphi K$ where

$$\varphi : K \to \mathrm{Aut}(H)$$
$$\varphi(y)(x) = yxy^{-1} \quad \forall x \in H, y \in K$$

Proof

Note: $\varphi(y) : H \to H$
$\varphi(y)(x) = yxy^{-1}$, since $H \lhd G$. $\varphi(y) = \psi_y|_H \in \mathrm{Aut}(H)$.
$\implies \varphi : K \to \mathrm{Aut}(H)$,

$$\varphi(yy') = \psi_{yy'|H} = (\psi_y \circ \psi_{y'})|_H = \psi_y|_H \circ \psi_{y'}|_H = \varphi(y) \circ \varphi(y')$$

Let us define $f : H \rtimes_\varphi K \to G$
$f(h,k) = hk$ for all $h \in H, k \in K$

f surjective because of (i)

$\ker(F) = \{1\}$:

$$hk = 1 \iff h = k^{-1} \in H \cap K \overset{\text{(ii)}}{=} \{1\} \implies h = 1, k = 1$$

f is a homomorphism:

$$\begin{aligned} f((h,k)(h',k')) &= f(h\varphi(k)(h'), kk') \\ &= h\varphi(k)(h')kk' \\ &= hkh'k^{-1}kk' \\ &= hkh'k' \\ &= f((h,k))f((h',k')) \end{aligned}$$

□

Remark: Equivalently,

$$G \cong H \rtimes K \iff \begin{cases} H \lhd G \\ K \subseteq G \xrightarrow[g]{} G/H \\ \text{is an isomorphism} \end{cases}$$

Proof
($\implies$) Proved.
($\impliedby$) Check (i)-(iii)

(ii) $\ker g = K \cap H$
g isomorphism $\implies K \cap H = \{1\}$

(iii) $H \lhd G$ by assumption.
g surjective $\implies \forall x \in G,\ \exists k \in K$ such that $g(k) = kH = xH$.

$$\begin{aligned} xk^{-1} \in H &\implies xk^{-1} = h \in H \\ &\implies x = hk \in HK \end{aligned}$$

□

Example 1.12.3
$D_{2n} \cong C_n \times C_2$.
$G = D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.
$H = \langle r \rangle$, $K = \langle s \rangle$, $H \cap K = \{1\}$, $H \lhd G$, $G = KH = HK$, since $G = HK \leq G$.

$$\implies G \cong H \rtimes K = C_n \rtimes C_2$$

$$\begin{aligned} \varphi : C_2 &\to \mathrm{Aut}(C_n) & \varphi(s)(r) &= r^{-1} \\ s &\mapsto (x \mapsto -x) & \varphi(s)(r^i) &= sr^i s^{-1} = sr^i s = r^{-i} \end{aligned}$$

Example 1.12.4
A_n = alternating group of even permutations.
$A_n = \ker(\varepsilon)$ where $\varepsilon : S_n \to \{\pm 1\}$. $A_n \lhd S_n$, $|S_n/A_n| = 2$.
$S_n \cong A_n \rtimes \langle \tau \rangle, \tau$ any transposition.
$K = \langle \tau \rangle,\ H = A_n \lhd S_n,\ H \cap K = \{1\},\ S_n = HK$.

$$\langle \tau \rangle \subseteq S_n \xrightarrow{\varepsilon} \{\pm 1\} \cong C_2 \qquad \varphi : C_2 \to \mathrm{Aut}(A_n),\ \varphi(\tau)(\sigma) = \tau\sigma\tau^{-1}$$
$$\cong$$

Example 1.12.5 (Non-example)
$Q \ncong$ semidirect product of $H, K \leq G, H, K \neq G$.
Assume

$$\left.\begin{array}{l} Q \cong H \rtimes K \\ H, K \neq G \end{array}\right\} \implies |H|, |K| \in \{2, 4\}$$

Remark: Any subgroup with 4 elements of Q is cyclic. (Q had only one element of order 2, namely -1)

$Q \ncong C_4 \rtimes_\varphi C_2$:

$$\varphi : C_2 \to \mathrm{Aut}(C_4) = (\mathbb{Z}/4\mathbb{Z})^\times = \{\widehat{1}, \widehat{3}\} \cong C_2$$
$$\mathrm{Aut}(C_4) = \{Id, x \mapsto -x\}$$

φ - nontrivial $\implies \varphi(\widehat{1})(\widehat{m}) = -\widehat{m}$, $\forall \widehat{m} \in C_4 = \mathbb{Z}/4\mathbb{Z}$.
If $Q \cong c_4 \rtimes_\varphi C_2$ for φ as above, then $Q \cong D_2$. Contradiction. D_8 has more elements of order 2.

Show: $Q \ncong C_2 \rtimes_\varphi C_4$.

$$\forall \varphi : C_4 \to \underbrace{\mathrm{Aut}(C_2)}_{(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}} = \{Id\}$$

$\implies Q \cong C_4 \times C_2$ which is abelian. Contradiction. □

Example 1.12.6
D_6 and C_6 are both semidirect products.
$C_6 \cong C_3 \times C_2$, $D_6 \cong C_3 \rtimes_\varphi C_2$. $(\mathbb{Z}/3\mathbb{Z})^\times = \{\widehat{1}, \widehat{2}\}$, $\mathrm{Aut}(C_3) = \{Id, x \mapsto -x\}$.
2 possibilities:

(i) $\varphi : C_2 \to \mathrm{Aut}(C_3)$
φ trivial $\implies C_6$

(ii) $C_2 \to \mathrm{Aut}(C_3)$
$T \mapsto (x \mapsto (x \mapsto -x)) \implies D_6$

Example 1.12.7
Dicyclic group: $m \geq 2$ integer

$$G = \{1, z, z^2, \ldots, z^{2m-1}, y, zy, \ldots, z^{2m-1}y\}$$

Multiplication:

$$\begin{aligned} z^a \cdot z^b &= z^{a+b} \\ z^a(z^b y) &= z^{a+b}y \\ (z^a y) \cdot z^b &= z^{a-b}y \qquad (*) \\ (z^a y)(z^b y) &= z^{a-b+m} \qquad (**) \end{aligned}$$

Exercise: Associativity holds for this multiplication.
Remark:

$$y^2 = z^m, \quad yz = z^{-1}y \qquad (*)$$

$$\mathrm{ord}(z) = 2m, \quad \mathrm{ord}(y) = 4 : \quad (z^m y)(z^m y) = z^m \qquad (**)$$

$\implies yz^m y = 1 \implies yz^m y^2 = y \implies z^{2m} = 1 = y^4 \implies y^2 = z^m$

$m = 2$: This is Q. $(z \mapsto i, y \mapsto j)$.
$m = 3$: This is $C_3 \rtimes_\varphi C_4$ (New group of order 12).

1.13 Examples of $H \rtimes K$

Example 1.13.1 (Dicyclic Group of order 12)
$G = \{1, z, z^2, \ldots, z^5, y, yz, \ldots, yz^5\}$.
$\mathrm{ord}(z) = 6$, $\mathrm{ord}(z) = 6$, $\mathrm{ord}(y) = 4$, $z^3 = y^2$, $zy = yz^{-1}$, $z^i y = yz^{-i}$.
Remark: G is nonabelian and $\mathrm{ord}(yz^i) = 4$

Claim: $G \cong C_3 \rtimes C_4$, $\varphi : C_4 \to \mathrm{Aut}(C_3) \cong C_2$, $\{Id, x \mapsto -x\}$

Proof of Claim:
φ nontrivial $\iff \varphi(\widehat{1})(x) = -x$

Let $H = \langle z^2 \rangle = \{1, z^2, z^4\}$, $K = \langle y \rangle = \{1, y, z^3, yz^3\}$

$H \cap K = \{1\}$, $G = HK$: $H \lhd G$, H is a characteristic subgroup since H is the only subgroup of G that has 3 elements.

$\implies G \cong H \rtimes_\varphi K$, G nonabelian $\implies \varphi$ nontrivial. ■

Remark (Prove later): $|G| = 12$, then G must be one of:

$C_3 \times C_4$, $C_3 \times C_2 \times C_2$ - abelian
A_4, D_{12}, $C_3 \rtimes_\varphi C_4$ - non-abelian

Elements of order 2:
$A_4 : 3$, $D_{12} :\geq 6$, $C_3 \rtimes_\varphi C_4 : 1$.
Remark: G group, $|G| = p^2$ (p odd prime) $\implies G \ncong H \rtimes_\varphi K$, $H, K \leq G, \varphi$ non-trivial.

$\forall C_p \rtimes_\varphi C_p$ has $\varphi =$ trivial

$$\varphi : C_p \to \mathrm{Aut}(C_p) \cong C_{p-1}$$

$\nexists$ non-trivial homomorphism $C_p \to C_{p-1}$.

$\forall f : C_p \to C_{p-1}$ has $\ker f = C_p$.
If $\ker f \neq C_p \implies \ker f = C_p \implies C_p \leq C_{p-1}$. Contradiction.

Groups of order p^3 (p odd prime)

Look at:
$C_{p^2} \rtimes C_p$
$(C_p \times C_p) \rtimes C_p$
$C_p \rtimes C_{p^2}$
$C_p \rtimes (C_p \times C_p)$

All $C_p \rtimes C_{p^2}$ is $C_p \times C_{p^2}$.

$\nexists$ non-trvial homomorphisms

$$C_{p^2} \to \mathrm{Aut}(C_p) \cong C_{p-1}$$

So all $C_p \rtimes (C_p \times C_p)$ is $C_p \times (C_p \times C_p)$.

$\nexists$ non-trivial homomorphism: $C_p \times C_p \to \mathrm{Aut}(C_p) \cong C_{p-1}$.

1.14 Examples of non-abelian groups G with p^3 elements

(i) $G = C_{p^2} \rtimes_\varphi C_p$, $\varphi =$ non-trivial

$$\varphi : C_p \to \mathrm{Aut}(C_{p^2}) \cong C_p \times C_{p-1}$$

All non-trivial $\varphi(C_p) \cong C_p \times \{1\}$
Claim 1: $\forall \varphi_1, \varphi_2$

$$C_{p^2} \rtimes_{\varphi_1} C_p \cong C_{p^2} \rtimes_{\varphi_2} C_p$$

Exercise: $G = \langle a, b \rangle$ where $\mathrm{ord}(a) = p^2$, $\mathrm{ord}(b) = p$, $bab^{-1} = a^{p+1}$.

(ii) $G = (C_p \times C_p) \rtimes_\varphi C_p$, $\varphi =$ non-trivial,

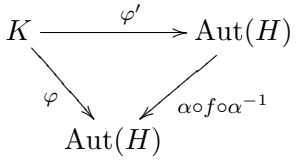
$$\varphi : C_p \to \mathrm{Aut}(C_p \times C_p) \cong GL_2(\mathbb{F}_p)$$

Claim 2: $\forall \varphi_1, \varphi_2$ nontrivial $\implies (Cp \times C_p) \rtimes_{\varphi_1} C_p \cong (C_p \times C_p) \rtimes_{\varphi_2} C_p$.

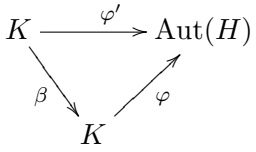
Example 1.14.1
$G = \langle a, b, c \rangle$, $\mathrm{ord}(a) = \mathrm{ord}(b) = \mathrm{ord}(c) = p$, $b = cac^{-1}a^{-1}$, $ba = ab$, $bc = cb$.

Criterion for $H \rtimes_\varphi K \cong H \rtimes_{\varphi'} K$:

(i) $\exists \alpha \in \mathrm{Aut}(H)$ such that the following diagram commutes:



(ii) $\exists \beta \in \mathrm{Aut}(K)$ such that the following diagram commutes:



(iii) K cyclic, $\varphi(K)$, $\varphi(K')$ are conjugate subgroups of $\mathrm{Aut}(H)$, i.e. $\exists \alpha \in \mathrm{Aut}(H)$ such that $\varphi'(K) = \alpha(\varphi(K))\alpha^{-1}$.

Claim: Claim 1 follows from (*iii*)
$\forall \varphi$, $C_p \to C_p \times C_p$ has $\varphi(C_p) = C_p \times \{1\}$, so $\forall \varphi_1 \varphi_2$ non-trivial, then $\varphi_1(C_p) \cong \varphi_2(C_p)$.

Claim: Claim 2 follows from (*iii*)
$\varphi : C_p \to GL_2(\mathbb{F}_p)$ Any two subgroups of order p of $GL_2(\mathbb{F}_p)$ are conjugate. (Theorem (Sylow): $|G| = p^n \cdot m$, $(m,p) = 1$, then any two subgroups of order p^n are conjugate)
$|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$:

$$GL_2(\mathbb{F}_p) = \{[\vec{a_1}, \vec{v_2}] \mid \vec{a_2} \text{ is not a multiple of } \vec{a_1}\}$$

# of choices for $\vec{a_1}$ is $p^2 - 1$.
# of choices for $\vec{a_2}$ is $p^2 - p$.

1.15 Classification of Groups of Order $2p, p^2, p^3$, p odd prime

Theorem 1.15.1
$|G| = 2p \implies G \cong C_{2p}$ or D_{2p}.

Proof
Cauchy's Theorem $\implies \begin{cases} \exists x \in G, \mathrm{ord}(x) = p \\ \exists y \in G, \mathrm{ord}(y) = 2 \end{cases}$

Let $H = \langle x \rangle$, $K = \langle y \rangle$. Then $H \cong C_p$, $K \cong C_2$.

$H \lhd G$ since $|G : H| = 2$.
$H \cap K = \{1\}$ by Langrange's Theorem (since p is odd). $H \lhd G \implies HK \leq G$.

Second isomorphism theorem $\implies$

$$HK/H \cong K/(H \cap K) \implies |HK| = |H||K| = 2p$$

$\implies G = HK \implies G \cong H \rtimes_\varphi K$, for some $\varphi : K \to \mathrm{Aut}(H)$.

Any hom $\varphi : C_2 \to \text{Aut}(C_p) \cong C_{p-1}$ is one of $\begin{matrix}\varphi = \text{ trivial} \\ \varphi(\widehat{1})(x) = x\end{matrix}$.

Use: C_{p-1} has a unique element of order 2: $\widehat{\frac{p-1}{2}}$ φ trivial $\implies G \cong C_p \times C_2$
$\varphi \neq$ trivial $\implies G \cong C_{2p}$. □

Theorem 1.15.2
$|G| = p^2 \implies G$ abelian and $G \cong C_p \times C_p$ or C_{2p}.

Proposition 1.15.3
$|G| = p^n \implies Z(G) \neq \{1\}$. (prove later)

Lemma 1.15.4
$G/Z(G)$ cyclic $\implies G$ abelian.

Proof
Denote $\widehat{x} = xZ(G) \in G/Z(G)$.
Let $G/Z(G) = \langle \widehat{x} \rangle$. Then any $\widehat{y} \in G/Z(G)$ is of the form $\widehat{y} = \widehat{x}^i \iff yx^{-1} \in Z(G)$.
So $\forall y \in G$ is of the form $y = x^i z$ for some $z \in Z(G)$.

Let $y_1, y_2 \in G$, then $y_1 = x^i z_1$, $y_2 = x^j z_2$ for some $Z_1, z_2 \in Z(G)$. Then $y_1 y_2 = x^i z_1 x^j z_2 = x^i x^j z_1 z_2 = x^j x^i z_2 z_1 = x^j z_2 x_i z_1 = y_2 y_1$. □

Proof of Theorem
$|G| = p^2$, $Z(G) \neq \{1\} \implies |Z(G)| = p$ or p^2.
If $|Z(G) = p$ then $G/Z(G)$ cyclic (has p elements).
$\implies G$ abelian, i.e., $G = Z(G)$. Contradiction.
Lemma $\implies |Z(G)| = p^2 \implies G = Z(G)$ □

p odd prime.

Theorem 1.15.5
If $|G| = p^3$, then either G is abelian, so isomorphic to

$$C_{p^3}, C_{p^2} \times C_p, C_p \times C_p \times C_p$$

or G is nonabelian, and is isomorphic to either

$$\begin{matrix} C_{p^2} \rtimes_\varphi C_p & \varphi \text{ nontrivial} \\ (C_p \times C_p) \rtimes_\varphi C_p & \text{(independent of } \varphi) \end{matrix}$$

$p = 2$, two nonabelian groups: D_8 and Q.

Two Facts:

(i) G p-group $\implies Z(G) \neq \{1\}$

(ii) G finite and p smallest prime such that $p \big| |G| \implies$ every subgroup of index p in G is normal.

Proof
Suppose G nonabelian, then $Z(G) \neq G$. Every element in G has order p or p^2.

Last time: $G/Z(G)$ cyclic $\implies$ G abelian.

So $G/Z(G)$ not cyclic. Therefore $|Z(G)| = p$, $|G/Z(G)| = p^2$ and $G/Z(G)$ not cyclic $\implies$ $G/Z(G) \cong C_p \times C - p$, by classification of groups of order p^2. So $x \in G \implies x^p \in Z(G)$.

Recall: Commutator subgroup $[G, G] = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$.

$$G/H \quad \text{abelian} \iff [G, G] \subseteq H$$

$G/Z(G)$ abelian $\implies [G, G] \subseteq Z(G)$.
$[G, G]$ non-trivial as G is nonabelian. $Z(G)$ order $p \implies [G, G] = Z(G)$.

Lemma 1.15.6
If $[G, G] \subseteq Z(G)$, then $\forall x, y \in G$,

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2} \qquad \forall n \in \mathbb{Z}$$

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

Example 1.15.7

$$\begin{aligned}(xy)^2 &= xyxy \\ &= xxy[y^{-1}x^{-1}yx]y \\ &= x^2y^2[y, x]\end{aligned}$$

$\phi : G \to Z(G), \phi(x) = x^p$,

$$(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$$

(pth power in $Z(G)$ and $|Z(G)| = p$).

Case 1:
$|\ker \phi| = p^2 \iff \phi$ surjective $\iff G$ has an element of order p^2.

$\exists x \in G$, $x^p \neq 1 \implies x$ has order p^2
$\exists y \in \ker \phi$ such that $y \notin \langle x \rangle$. y has order p. Let $H = \langle x \rangle \cong C_{p^2}$ and $K = \langle y \rangle \cong C_p$.
$[G : H] = p \implies H \trianglelefteq G$. $H \cap K = \{e\} \implies HK = G \implies G \cong H \rtimes_\varphi K$, φ nontrivial.

Case 2
$|\ker \phi| = p^3 \iff \phi$ triv $\iff G$ has exponent p.

Let x be a generator of $Z(G)$. $|\langle x \rangle| = |Z(G)| = p$

$$G \to G/Z(G) \cong C_p \times C_p$$

Choose y and $z \in G$ that map to $(0, 1)$ and $(1, 0)$ under this map.

$H = \langle x, y \rangle$, $K = \langle z \rangle$.

- H does not surject onto $G/Z(G)$, so $H \neq G$. $g \notin \langle x \rangle$ so $|H| > p$. So $|H| = p^2$ and $|K| = p$. $[G : H] = p \implies H \trianglelefteq G$.
- $H \cap K = \{1\}$.
- Suppose $y^i x^j = z^l$, $y^i Z(G) = z^l Z(G) \implies i, l \equiv 0 \bmod p. \implies i, j, k \equiv 0 \bmod p. \implies HK = G$

$\implies H \rtimes_\varphi K \cong G$. $\square$

Example 1.15.8

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/p^2\mathbb{Z}) \mid a \equiv \mod p, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}$$

Example 1.15.9

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{Z}/p\mathbb{Z}) \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

1.16 Group Actions

Definition 1.16.1
G group, X set.
A left action of G on X is a map

$$G \times X \to X \qquad (g, x) \mapsto g \cdot x$$

such that

(i) $1 \cdot x = x \quad \forall x \in X$

(ii) $g \circ (h \cdot x) = (gh) \cdot x \quad \forall g, h \in G, x \in X$

X is called a (left) G-set.
$g \in G$, $t_g : X \to X$, $t_g(x) = g \cdot x$ left translation by g, $t_{g-1} = (tg)^{-1}$.

Example 1.16.2
G acts on G by left multiplication: $G \times G \to G$, $(g, h) \mapsto g \cdot h$.
$t_g(h) = g \cdot h$, $t_g \in S_X$.
$S_X = \{f : X \to X \mid f \text{ is a bijection}\}$ symmetric group on X.

Homomorphism:
$G \to S_X$, $g \mapsto t_g$, $gh \mapsto t_{gh}$:

$$\begin{aligned} t_{gh}(x) &= (gh) \cdot x \\ &= g \cdot (h \cdot x) \\ &= g \cdot t_h(x) \\ &= t_g(t_h(x)) \end{aligned}$$

Given hom $f : G \to S_X$ define:

$$G \times X \to X \text{ by } (g, x) \mapsto f(g)(x)$$

(i) $(e, x) \mapsto f(e)(x) = id(x) = x$

(ii) $g(h \cdot x) = f(g)(h \cdot x) = f(g)(f(h)(x)) = (f(g) \circ f(h))(x) = f(gh)(x) = (gh)x$

{Left G-actions on X}$\leftrightarrow$ {permutation representation $G \to S_X$}

Definition 1.16.3
An action G on X is <u>faithful</u> if its permutation representation $G \to S_X$ is injective. $\iff$ for each $g \in G \setminus \{1\}$, $\exists x \in X$ such that $gx \neq x$.

Exercise: S_X acts on X, $\sigma \in S$, $x \in X$, $\sigma \cdot x = \sigma(x)$.
Exercise: $G \leq S_X$ $G \hookrightarrow S_X$ faithful since if $\sigma \neq 1$, then $\exists x \in X$ such that $\sigma(x) \neq x$.

Example 1.16.4
$H \leq G$, H acts on G by left multiplication $H \times G \to G$, $(h, g) \mapsto hg$.
If $h \neq 1$, then $h \cdot g \neq g \ \forall g \in G$.
So faithful $\implies$ $H \hookrightarrow S_G$.

Theorem 1.16.5
(Cayley's Theorem) Every group is isomorphic to a subgroup of a symmetric group.

Proof
$H = G$ in last example $\implies$ $G \in S_G$. □

Example 1.16.6
$H \leq G$. Then G acts on the quotient G/H

$$g \cdot (xH) = (gx)H$$

Not faithful if $H \neq 1$.

Example 1.16.7
G acts on G by conjugation,

$$G \times G \to G$$
$$(g, x) \mapsto gxg^{-1}$$
$$ghx(gh)^{-1} = g(hxh^{-1})g^{-1}$$

is a left action.

Example 1.16.8
G acts on the set of subgroups of G by conjugation. $(g, H) = gHg^{-1}$.

Example 1.16.9
$N \trianglelefteq G$, G acts on N by conjugation, $(g, n) \mapsto gng^{-1}$.
G acts on G/N by conjugation, $(g, xN) \mapsto gxg^{-1}N$.

1.17 Examples of Actions G on X

(i) S_n acts on $X = \{1, 2, \ldots, n\}$

(ii) $G \times G \to G$, $(g, x) \mapsto gx$

(iii) $H \leq G$, G/H = left cosets of H in G

$$G \times G/H \to G/H, \quad (g, xh) \mapsto g \times H$$

(iv) $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$

(v) $N \triangleleft G$, $G \times N \to N$, $(g, x) \mapsto gxg^{-1}$

$$G \times G/N \to G/N, \quad (g, \widehat{x}) \mapsto g\widehat{x}g^{-1}, \quad \widehat{x} = xN$$

(vi) G acts on $\{\text{subgroups of } G\}$, $(g, H) \mapsto gHg^{-1}$

(ii) (iii) left multiplication, (iv)-(vi) conjugation.

Example 1.17.1
G group, $\mathrm{Aut}(G)$ acts on G: $(f, x) \mapsto f(x)$.

$G =$ group of isometries of $\mathbb{R}^n$ (bijective $f : \mathbb{R}^n \to \mathbb{R}^n$), preserving distance, G acts on $\mathbb{R}^n$, $f \cdot x = f(x)$.

1.18 Orbits

Let G acts on X.

Definition 1.18.1
A subset $S \subseteq X$ is stable under the action of G if $\forall g \in G$, $\forall x \in S$, $g \cdot x \in S$.
If S is stable under the action of G on X, then G acts on S.

Definition 1.18.2
Let $x \in X$.

$$\mathcal{O}(x) = \{g \cdot x \mid \forall g \in G\}$$

(Gx) - orbit of x (smallest S such that $x \in S$ and S is G-stable).

Lemma 1.18.3
Let X be a G-set. The relation(defn) $x \sim y \iff \exists g \in G$ such that $y = gx$ is an equivalence relation.
The equivalence class of x is $\mathcal{O}(x) = \{y \in X \mid y \sim x\}$.

Corollary 1.18.4
Distinct orbits form a partition of X.

Definition 1.18.5
The action is called transitive if $\exists$ just one orbit.

Example 1.18.6
S_n acting on $\{1, \ldots, n\}$ is transitive.
For all $i, j \in \{1, \ldots, n\}$, let $\alpha = (i\ j)$, $\alpha \cdot i = \alpha(i) = j$

Example 1.18.7
$G \times G \to G$, $(g, x) \mapsto gx$ is transitive

Example 1.18.8
$G \times G/H \to G/H$, $(g, xH) = g \times H$ is transitive

Example 1.18.9
$G \times G \to G$, $(g, x) \mapsto gxg^{-1}$
Orbits - conjugacy classes

$$\mathcal{O}(x) = \{gxg^{-1} \mid g \in G\} \quad \text{- conjugation of } x$$

Remark:

- $\mathcal{O}(x) = \{x\} \implies x \in Z(G)$.

$$\begin{aligned}\mathcal{O}(x) = \{gxg^{-1} \mid g \in G = \{x\} \\ &\iff gxg^{-1} = x \quad \forall g \in G \\ &\iff gx = xg \quad \forall g \in G \\ &\iff x \in Z(G)\end{aligned}$$

- This is not a transitive action if $G \neq \{1\}$.
- Conjugacy classes in $GL_n(\mathbb{F}) =$ <u>similarity classes</u>
- A subset S is G-stable $\iff$ S is a union of orbits.
  A subgroup H of G is <u>normal</u> $\iff$ H is stable under the action by conjugation:

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}$$

  $\implies$ H is normal in G $\iff$ H is a union of conjugacy classes.

1.19 Stabilisers

G acts on X, $x \in X$, the stabliliser of x is

$$\text{Stab}(x) = G_x = \{g \in G \mid gx = x\} \subseteq G$$

and is a subgroup of G.
$g \in G_x \implies g^{-1} \in G_x : gx = x \iff x = g^{-1}x$
$g, h \in G_x \implies gh \in G_x : (gh)x = g \cdot (hx) = gx = x$

Example 1.19.1
S_n acts $X = \{1, \ldots, n\}$.

$$i \in X : G_i = \{\alpha \in S_n \mid \alpha(i) = i\} = \text{permutations of } X \setminus \{i\} \cong S_{n-1}$$

Example 1.19.2
$H \leq G$, $H \times G \to G$, $(h, x) = hx$. $x \in G$, $G_x = \{h \in H \mid h\cancel{x} = \cancel{x}\} = \{1\}$.

Example 1.19.3

$$\begin{aligned}G_{xH} &= \{g \in G \mid gxH = xH\} \\ &= \{g \in G \mid x^{-1}gx \in H\} \\ &= xHx^{-1}\end{aligned}$$

Example 1.19.4
$G \times G \to G$, $(g, x) \mapsto gxg^{-1}$,

$$G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$$

This is the <u>centraliser of x</u>

$$C_G(x) := \{g \in G \mid gx = xg\} = N_G(x)$$

Definition 1.19.5
$A \subseteq G$ subset. The centraliser of A is

$$C_G(A) = \{g \in G \mid ga = ag \quad \forall a \in A\}$$

Recall: $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$
Remark:

- $Z(G) \subseteq C_G(A) \subseteq N_G(A)$.
- $Z(G) = \bigcap_{x \in G} C_G(x)$

Example 1.19.6
G = group of isometries of $\mathbb{R}^n$, G acts on $\mathbb{R}^n$. Stabiliser of $0 \in \mathbb{R}^n$, $G_0 = O_n(\mathbb{R})$

$H \lhd G \iff N_G(H) = G$.

Example 1.19.7
G acts on {subgroups of G}, $(g, H) \mapsto gHg^{-1}$.

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

Let $T \subseteq G$ be the subgroup

$$T = \{t_v \mid t_v(x) = x + v\} \qquad \text{- translation by } v$$

Exercise: $T \lhd G$, $G \cong T \rtimes O_n(\mathbb{R})$.
Remark:

- $O_n(\mathbb{R}) \not\lhd G$: $f \in O_n(\mathbb{R})$. $f(x) = Ax$, $A \in O_n(\mathbb{R})$. Note that $t_v^{-1} = t_{-v}$,

  $$t_v \circ f \circ t_v^{-1}(x) = A(x - v) + v = Ax + v - Av \neq Ax$$

  $\implies t_v \circ f \circ t_v^{-1} \neq f$ in general.
- $G_x \not\lhd G$ in general for G acting on X. $G_{xy} = xG_yx^{-1}$.
  $g \in G_{xy} \iff g(xy) = xy \iff (x^{-1}gx)y = y \iff x^{-1}gx \in G_y$.
- $$\bigcap_{x \in G} G_x = \ker(G \to S_x) = \{g \in G \mid t_g = Id_x, gx = x \quad \forall x \in X\}$$

G acts on X faithfully $\iff \bigcap_{x \in G} G_x = \{1\}$.

Theorem 1.19.8
G a group, $H \leq G$. G/H = left cosets of H in G. G acts on G/H by $(g, xH) = gxH$. Let $\pi_H : G \to S_{G/H}$ be the associated permutation representation. Then:

(i) G acts transitively on G/H

(ii) $G_H = H$

(iii) $\ker(\pi_H) = \bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup of G contained in H.

Proof

(i) Already proved

(ii) Recall $G_{xH} = xHx^{-1} \implies G_H = H$

(iii) Remark $\implies \ker(\pi_H) = \bigcap_{x\in G} G_{xH} = \bigcap_{x\in G}(xHx^{-1}) \implies$ normal in G (kernel of π).
Let $N \lhd G$, $N \subseteq H$. Prove $N \subseteq \ker(\pi_H) = \bigcap_{x\in G} xHx^{-1}$. Show $\forall x \in G, N \subseteq xHx^{-1}$.
But $x^{-1}Nx \underset{\text{normal}}{\subseteq} N \subseteq H \implies N \subseteq xHx^{-1}\ \forall x \in G$.

□

Remark:

- If H contains no non-trivial normal subgroup of G, then

$$\pi_H : G \to S_{G/H} \quad \text{is injective.}$$

  Cayley's theorem: $H = \{1\} : G \to S_G$ is injective. For example if G is simple.

- If $|G|$ does not divide $|G : H|!$, then G cannot be simple.

Example 1.19.9
$|G| = 99$, $H = \langle x\rangle$ for some $x \in G$, $\text{ord}(x) = 11$.

$$\pi_H : G \to S_{G/H} = S_9, \quad 99 \nmid 9!$$

$\ker(\pi_H) \subseteq H$ (largest) normal subgroup of G contained in H.
$\implies \ker(\pi_H) \neq \{1\}$ (since $99 \nmid 9!$)
$\implies \ker(\pi_H) = H \lhd G$.

Corollary 1.19.10
G finite group of order n. $p =$ smallest prime such that $p|n$. Then $\forall H \leq G$, $|G : H| = p$ is normal.

Proof
$\pi_H : G \to S_{G/H} \cong S_p$. Let $K = \ker \pi_H$.
By theorem, $K \lhd G$, $K \subseteq H$, so have $K \subseteq H \subseteq G$. $|G : K| = |G : H||H : K|$.
Let $k = |H : K|$. Then $|G : K| = pk$.
$K = \ker \pi_H \implies G/K \to S_p$ is injective, $\implies pk = |G/K|$ divides $p! \implies k|(p-1)!$. $k = |H : K|$ divides $|H|$, $|G| = n$. $p =$ smallest prime dividing $n \implies k = 1$ or $\exists q$ prime $q|K$.
But $k|(p-1)! \implies k = 1 \implies K = H \lhd G$. □

Theorem 1.19.11
Let G act on X, $x \in X$. Then $\exists$ bijection

$$f : \mathcal{O}(x) \to G/G_x$$
$$f(g \cdot x) = gG_x$$

In particular, $|\mathcal{O}(x)| = |G : G_x|$.

Proof
f surjective: Clear.
f injective:

$$gG_x = hG_x \iff g^{-1}h \in G_x \iff (g^{-1}h) \cdot x = x \iff h \cdot x = g \cdot x.$$

□

Corollary 1.19.12
If $|G| < \infty$, then $|\,\mathcal{O}(x)| = \frac{|G|}{|G_x|}$ so $|G| = |\,\mathcal{O}(x)||G_x|$.

Corollary 1.19.13
- The number of conjugates gxg^{-1} of $x \in G$ is $|G : C_g(x)|$.
- The number of conjugates gHg^{-1} of $H \leq G$ is $|G : N_G(H)|$.

Recall: Disjoint orbits form a partition of X for any action G on X.
Consequence: G acts on X, G finite,

$$|X| = \sum_{\substack{\text{disjoint} \\ \text{orbits}}} |\text{orbit } \mathcal{O}(x)| = \sum_{\substack{\text{disjoint} \\ \text{rep } x}} \frac{|G|}{|G_x|}.$$

The Class Equation

$$|G| = \sum_{\substack{\text{disjoint} \\ \text{rep } x}} |G : C_g(x)| = |Z(G)| + \sum_{\substack{\text{rep. } y \\ \text{of order} > 1}} |G : C_g(y)|$$

Use:

$$\mathcal{O}(x) = \{x\} \iff z \in Z(G)$$
$$\mathcal{O}(x) = \{x\} \iff C_G(x) \text{ is a proper subgroup of } G$$

Theorem 1.19.14 (Cauchy's Theorem)
If the prime p divides $|G| < \infty$ then G contains an element of order p

Proof
Induction on $|G|$:
If $\exists y \notin Z(G)$ such that $p \nmid |G : C_g(y)|$ then $p \big| |C_G(y)|$.
$y \notin Z(G) \iff C_g(y) < G$ proper subgroup.
If $p \big| |C_g(y)|$ and $y \notin Z(G)$, done by induction. □

Claim: Cauchy's Theorem is true for abelian groups Z.

Proof
Induction on $|Z|$:
Enough to find $z \in Z$ such that $p \big|\, \text{ord}(x)$.
If $\text{ord}(x) = pk$, then $\text{ord}(x^k) = p$.
Pick any non-trivial $x \in Z$. If $p \big|\, \text{ord}(x)$, done.
Assume $p \nmid \text{ord}(x)$. Then $p \big| |Z/\langle x \rangle|$. By induction, $\exists \widehat{y} \in \mathbb{Z}/\langle x \rangle \ni \text{ord}(\widehat{y}) = p$.
Let $l = \text{ord}(y)$, then $y^l = 1 \implies \widehat{y}^l = 1 \implies p \big| d$. □

Theorem 1.19.15
If $|G| = p^n$, then $Z(G)$ is non-trivial.

Proof
If $y \notin Z(G)$, then

$$C_g(y) < G \implies p \big| |G : C_g(y)| = \frac{|G|}{|C_g(y)|}.$$

By class equation, $p \big| |Z(G)|$. □

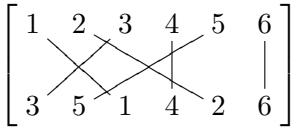
1.20 Presentations

Definition 1.20.1
If $\alpha = \begin{bmatrix} 1 & \dots & n \\ \alpha(1) & \dots & \alpha(n) \end{bmatrix}$, then the pair (i,j) is an inversion of α if $\alpha(i) > \alpha(j)$ when $i < j$.
α is even (odd) if the number of inversions of α is even (odd).
Define

$$\operatorname{sgn}(\alpha) \text{ or } \varepsilon(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

Example 1.20.2

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 2 & 6 \end{bmatrix}$$



inversions = # crossings.

Proposition 1.20.3
$\varepsilon : S_n \to \{\pm\}$ is a group homomorphism.

Proof
Let $x_1, \dots, x_n$ be variables. For every polynomial Q in $x_1, \dots, x_n$ and $\alpha \in S_n$, define:

$$\alpha Q := \text{ polynomial obtained from } Q \text{ by } x_i \mapsto x_{\alpha(i)}$$

Let $P = (x_2 - x_1)(x_3 - x_1)\cdots(x_n - x_1)(x_3 - x_2)\cdots(x_n - x_{n-1})$

Claim 1: $\alpha(P) = \varepsilon(\alpha)P$
Claim 2: $\beta(\alpha(P)) = (\beta\alpha)(P)$

$$\begin{aligned} \beta(\alpha(P)) : x_i &\mapsto x_{\alpha(i)} \\ x_k &\mapsto x_{\beta(k)} \qquad \forall k \end{aligned}$$

which is $(\beta\alpha)(P)$. ■
Thus,

$$\begin{aligned} \varepsilon(\beta\alpha)(P) = (\beta\alpha)(P) = \beta(\alpha(P)) = &\beta(\varepsilon(\alpha)P) = \varepsilon(\alpha)\beta(P) = \varepsilon(\alpha)\varepsilon(\beta)(P) \\ &\implies \varepsilon(\beta\alpha) = \varepsilon(\beta)\varepsilon(\alpha) \end{aligned}$$

□

Definition 1.20.4
$A_n = \ker(\varepsilon)$.
So $A_n \lhd S_n$. In fact, $|S_n : A_n| = 2$ for $n \geq 2$ by first isomorphism theorem since ε is surjective.
Exercise: $\varepsilon(ij) = -1$.

Theorem 1.20.5
Every $\alpha \in S_n$ is a product of disjoint cycles and is unique upto reordering.

Proof
Let $\alpha \in S_n$. Let $H = \langle\alpha\rangle \leq S_n$. Consider the action H on $X = \{x_1, \dots, x_n\}$.
Then the orbits have the form $\mathcal{O}(i) = \{i, \alpha(i), \dots, \alpha^{r-1}(i)\}$ where $r = \min\{k \mid \alpha^k(i) = i\}$.

Note that $|\mathcal{O}(i)| = r$. To $\mathcal{O}(i)$, associate γ by $\gamma_i(i, \alpha(i), \alpha^2(i), \ldots, \alpha^{r-1}(i))$. Then $\forall x \in \mathcal{O}(i)$, $\alpha(x) = \gamma_i(x)$.

Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ be all distinct orbits of H acting on X. Then

$$X = \bigsqcup_{j=1}^{m} \mathcal{O}_j$$

Note that $\gamma_1, \ldots, \gamma_m$ are disjoint cycles and length$(\gamma_i) = |\mathcal{O}_i|$.

Claim: $\alpha = \gamma_1 \cdots \gamma_m$

Proof of Claim:
Let $i \in \mathcal{O}_k$. Then $\alpha(i) = \gamma_k(i) = \gamma_1 \cdots \gamma_m(i)$. ■

Uniqueness: Any decomposition $\alpha = \gamma_1 \cdots \gamma_m$, disjoint cycles gives a partition of X into orbits for $H = \langle \alpha \rangle$ acting on X. □

Corollary 1.20.6
$\forall \alpha \in S_n$, α is a product of transpositions.

Corollary 1.20.7
A_n, $n \geq 3$, then A_n is generated by 3-cycles.

Proof
$\forall \alpha \in A_n$, α is a product of an even number of transpositions. Any $(i\ j)(k\ l)$ is a product of 3-cycles.

$$(i\ j)(k\ l) = \begin{cases} (i\ j\ k) & \text{if } k = j \\ (i\ j\ k)(j\ k\ l) & \text{if } \{i, j, k, l\} \\ 1 & \text{if } \{i, j\} = \{k, l\} \end{cases}$$

□

1.21 Conjugacy Classes in S_n

Remark: If $\alpha \in S_n$, then $\alpha(a_1\ \ldots\ a_k)\alpha^{-1} = (\alpha(a_1)\ \alpha(a_2)\ \ldots\ \alpha(a_k))$.

Lemma 1.21.1
Any two k-cycles are conjugate.

Proof
Let $u = (a_1\ \ldots\ a_k)$ and $v = (b_1\ \cdots\ b_k)$.
Define $\alpha \in S_n$ by $\alpha(a_i) = b_i\ \forall i$ and send $\alpha(x)$ to something not b_i for each $x \neq a_i$, no repeating. □

Definition 1.21.2
A partition of n is a sequence of integers $1 \leq n_1 \leq n_2 \leq \ldots \leq n_k \leq n$ such that $n_1 + \cdots + n_k = n$.
If $\alpha = \gamma_1 \cdots \gamma_m$ disjoint cycles then this gives a partition of $n = \sum_{i=1}^{m} \text{length}(\gamma_i)$.

Proposition 1.21.3
Two elements $\alpha, \beta \in S_n$ are conjugate iff α and β define the same partition of n.

Proof
$\alpha = \gamma_1 \cdots \gamma_m$, $\beta = \gamma_1' \cdots \gamma_m'$, length$(\gamma_i)$ =length(γ_i'). □

————Aside————

Application: Homework Q5-6.
$|G| = 2k$, k odd $\implies \exists H \leq G$, $|G : H| = 2$.
$G \xrightarrow{\pi} S_G$ by left multiplication $g \mapsto (x \mapsto gx) = \sigma_g$.

Claim: $\text{ord}(g) = 2 \implies \pi(g) =$ product of k disjoint transpositions.
Remark: If $g \neq 1 \implies gg_i \neq g_i$, $\text{ord}(g) = 2 \implies (\sigma_g)^2 = 1 \implies \text{ord}(\sigma_g) = 2$.
σ_g is a product of disjoint transpositions (product of (g_i, gg_i)).

$G \xrightarrow{\pi} S_{2k}$, $\pi(G) \not\subseteq A_{2k}$. Let $H = \pi^{-1}$.
$G/H \to S_{2k}/A_{2k}$. $G \xrightarrow{f} G'$, $1 \to G/f^{-1}(H') \to G' \to G'/H' \to 1$.
————————————

Corollary 1.21.4
$Z(S_n) = \{1\}$.

Proof
G acts on G, $g \mapsto (x \mapsto gxg^{-1})$.
Orbits

$$\mathcal{O}(x) = \{gxg^{-1} \mid g \in G\}, \quad \mathcal{O}(x) = \{x\} \iff x \in Z(G)$$

$\alpha \in S_n$ is an $Z(S_n) \iff$ #of conjugacy class of $\alpha = 1$, only $\alpha = 1$. □

Application: For $\alpha \in S_n$, $\alpha = m$=cycle $(a_1, \ldots, a_m), (m \leq n)$.
Compute (i) # of conjugates of α, (ii) $C_{S_n}(\alpha)$.

(i) # of conjugates of $\alpha = \#m$-cycles in $S_n = \frac{n \cdot (n-1) \cdots (n-m+1)}{m}$

(ii) $C_G(x) =$ stabiliser G_x for G acting on G by conjugation, $|G| = |\mathcal{O}(x)||G_x|$

$$|C_{S_n}(\alpha)| = \frac{|S_n|}{\#\text{ conjugates of } \alpha} = \frac{n!}{\frac{n!}{(n-m)!m}} = m(n-m)!$$

Corollary 1.21.5
If $\alpha = (a_1 \ \cdots \ a_m)$ an m-cycle, then

$$C_{S_n}(\alpha) = \{\alpha^i \beta \mid 0 \leq i < m, \beta \in S_X\}$$

where $X = \{1 \cdots m\} \setminus \{a_1 \cdots a_m\}$.

Proof
Clearly, $\alpha^i \beta \in C_{S_m}(\alpha)$, $\forall i, \beta \in S_n$.

$$\text{Count: \# elements in RHS} = \text{internal direct product of } \langle \alpha \rangle, S_X$$

$\implies$ # elements in RHS $= (n-m)!m$. □

1.22 Conjugacy Classes in A_n

In S_4:= $\big\{\{Id\}, \{(i\ j)\}, \{(i\ j\ k)\}, \{(i\ j\ k\ l), (i\ j)(k\ l)\}\big\}$

In A_4: $\{Id\}, \{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\}, \{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}$ and $\{(i\ j)(k\ l)\}$.

In A_5: $\{Id\}, \{(i\ j\ k)\}, \{(ij)(kl)\}, \{(1\ 2\ 3\ 4\ 5), \ldots\}, \{(1\ 5\ 4\ 3\ 2), \ldots\}$

Claim: α 3-cycle, # conjugates of α in $A_5 = 20$:

$$\#\text{ conjugates of } \alpha = \frac{|G|}{|C_G(\alpha)|} = \frac{|A_5|}{|C_G(\alpha)|} = \frac{60}{|C_G(\alpha)|}$$

Proof
$\langle\alpha\rangle = C_G(\alpha)$, so $|C_G(\alpha)| = 3$.
Let $\beta \in C_G(\alpha)$, then $\beta\alpha\beta^{-1} = \alpha$.

Let $\alpha = (i\ j\ k)$, then $\beta(i\ j\ k)\beta^{-1} = (\beta(i)\beta(j)\beta(k))$

$$(\beta(i)\beta(j)\beta(k)) = (i\ j\ k) \iff \beta = Id \quad \text{or} \quad \beta = (i\ j\ k)(= \alpha) \quad \text{or} \quad \beta = (i\ k\ j)(= \alpha^2)$$

□

Example 1.22.1
$\alpha =$5-cycle $\implies$ # conjugates of $\alpha = \frac{60}{5} = 12$
5-cycles in $S_5 = 4! = 24$.

Example 1.22.2
$(1\ 2\ 3\ 4\ 5), (2\ 1\ 3\ 4\ 5)$ are not conjugate in A_5.

Corollary 1.22.3
A_5 is simple.

Proof
If $N \lhd A_5$, then $H =$ union of conjugacy classes. No pair of $\{1, 20, 15, 12, 12\}$ sums to a divisor of 60. □

Theorem 1.22.4
A_5 is simple for all $n \geq 5$.

Proof
We will take the following steps:

1. A_n is generated by 3-cycles
2. If $H \lhd A$ and H contains a 3-cycle, then H contains all 3-cycles.
3. $\forall H \leq A_n$, $n \geq 5$, non-trivial, H contains a 3-cycle

2. Let $\gamma = (i\ j\ k) \in H'$. Let $\beta = (a\ b\ c)$, $\exists\alpha \in S_n$, $\alpha\gamma\alpha^{-1} = \beta$.
If $\alpha \in A_n$, done (since H is normal).
Assume $\alpha \notin A_n$. Pick $t =$ transposition is S_n such that t disjoint from β, $(n \geq 5)$.
Then $t\alpha \in A_n$ and $\beta = t\beta t^{-1} = t(\alpha\gamma\alpha^{-1})t^{-1} = (t\alpha)\gamma(t\alpha)^{-1}$.

3. Let $H \lhd A_n$, $H \neq \{1\}$. Let $\alpha \in H, \alpha \neq 1$ not a 3-cycle. Then α has one of the following forms:
(i) $\alpha = (i_1\ i_2\ i_3 \cdots)(\cdots)$
(ii) $\alpha = (i_1\ i_2)(i_3\ i_4)\cdots$ disjoint

Construct $\alpha' \in H$ such that α' fixes more elements from $\{1, \ldots, n\}$ than α.

Case (i) $\alpha \neq (i_1\ i_2\ i_3)(i_1\ i_2\ i_3\ i_4)$ (not in A_4)
$\implies$ α moves two numbers other than i_1, i_2, i_3.

Let $\gamma = (i_3\ i_4\ i_5) \in A_n$.
Let $\alpha_1 = \gamma\alpha\gamma^{-1} \in H$, $(H \lhd A_n)$.
Let $\alpha' = \alpha_1\alpha^{-1}$. Then $\alpha' \in H$.

Claim: α' fixes i_2 and all elements fixed by α, $(u \neq i_1, \ldots, i_5)$

Proof of Claim:

$$\begin{aligned}\alpha'(i_2) &= \gamma\alpha\gamma^{-1}\alpha^{-1}(i_2) = \gamma\alpha\gamma^{-1}(i_1)\\ &= \gamma\alpha(i_1) = \gamma(i_2) = i_2\\ \gamma'(u) &= \gamma\alpha\gamma^{-1}\alpha^{-1}(u) = \gamma\alpha(u) = \gamma(u) = u\end{aligned}$$ ■

Case 2: Form $\gamma, \alpha_1, \alpha'$ as before with i_4 as in u and $i_5 \neq i_1, \ldots, i_4$.

Claim: $\alpha' = (\gamma\alpha\gamma^{-1}\alpha^{-1})$ fixes i_1, i_2, and $u \neq i_1, \ldots, i_5$

Proof of Claim:
Omitted. ■

□

Corollary 1.22.5
$Z(A_n) = \{1\}$ if $n \geq 5$.

Corollary 1.22.6
If $n \geq 5$, then the only normal subgroups of S_n are $\{1\}$, A_n ad S_n.
Remark: H = Klein subgroup in A_n, H characteristic in A_4. H characteristic in K, $K \lhd G \implies H \lhd G \big| H \lhd S_4$.

Proof Corollary
Let $H \lhd S_n$, $H \neq \{1\}$ or S_n. Then $H \cap A_n \lhd A_n$.
Theorem $\implies$ $H \cap A_n$ is $\{1\}$ or A_n. If $H \cap A_n = A_n \implies A_n \leq H$.
$\implies$ $H = A_n$ (since $|S_n : A_n| = 2$).

If $H \cap A_n = \{1\}$, $S_n \supseteq H \xrightarrow{f} S_n/A_n \cong C_2$.
Then $H \cap A_n = \{1\} \iff \ker f = \{1\}$.
$\implies \exists$ injective map $f : H \to C_2 \implies |H| = 2$.
If $H \neq \{1\}$, $|H| = 2 \implies \alpha \in H$ with $|\alpha| = 2 \implies (a_1\ a_2) = \alpha$ not normal. □

1.23 More Actions

G acts on subgroups of G by conjugation: $(x, H) \mapsto xHx^{-1}$.
Remark: $\psi_x : G \to G$, $\psi_{x|_H} : H \mapsto xHx^{-1}$ is an isomorphism. $|H| = |xHx^{-1}|$.

Stabiliser $G_H = \{x \in G \mid xHx^{-1} = H\} = N_G(H)$
$H \subseteq N_G(H) \subseteq G$, $N_G(H)$ is the largest subgroup of G in which H is normal.
Fact: # conjugates of $H = |G : N_G(H)|$. $(|\mathcal{O}(x)| = |G : G_x|)$

Example 1.23.1
$G = S_p$, p prime.
If H_p of order p, $(H = \langle\alpha\rangle$, $\alpha = p$-cycle), then $|N_{S_p}(H)| = p(p-1)$.

Proof
$|N_{S_p}(H)| = \frac{|S_p|}{\#\text{ conjugates of } H}$.

$$\#\text{ conjugates of } H = \frac{\#\ p\text{-cycles in } S_p}{\#\ p\text{-cycles in } H} = \frac{(p-1)!}{p-1} = (p-2)!$$

So

$$\frac{p!}{(p-2!)} = p(p-1) = |N_{S_p}(H)|.$$

□

Remark: $H = \langle\alpha\rangle$, $\alpha = p$-cycle, $H \leq C_{S_p}(H) \leq N_{S_p}(H)$.

Recall: $|C_{S_n}(\alpha)| = (n-m)!m$.
In particular, if $\alpha = p$-cyclic in S_p, then $C_{S_p}(\alpha) = \langle\alpha\rangle$. So

$$|N_{S_p}(\langle\alpha\rangle)/C_{S_p}(\langle\alpha\rangle)| = p-1.$$

If $H \lhd G$, then G acts on H by conjugtion $(g,x) \mapsto gxg^{-1}$. Associated presentation representation: $\varphi : G \to \mathrm{Aut}(H), \varphi(g) = \psi_{g|_H} : H \to H$.

Proposition 1.23.2
$\ker(\varphi) = C_G(H)$.

Proof
$\ker(\varphi) = \{g \in G \mid gxg^{-1} = x \quad \forall x \in H\} = C_G(H)$. □

Corollary 1.23.3
$G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular,

$$N_G(H)/C_G(H) \leq \mathrm{Aut}(H).$$

Remark: If $H = G$, $C_G(G) = Z(G) \implies G/Z(G) \leq \mathrm{Aut}(G)$. This is $\mathrm{Inn}(G)$.

Example 1.23.4
S_p, p prime, $\alpha = p-$cycle.

$$N_{S_p}(\langle\,\alpha\,\rangle)/C_{S_p}(\overline{\alpha}\,\rangle) \cong \mathrm{Aut}(\langle\,\alpha\,\rangle) = \mathrm{Aut}(C_p) \cong C_{p-1}$$

Example 1.23.5
$|G| = 203 = 7 \cdot 29$.
Assume G has a normal subgroup H, $|H| = 7$. Then

- $H \subseteq Z(G)$
- G is abelian.

Proof
Let $\varphi : G \to \mathrm{Aut}(H)$ as before. Then φ must be trivial since $(203, 6) = 1$.
$\implies \ker\varphi = G$, but $\ker\varphi = C_G(H)$. So $H \subseteq Z(G)$.

Want to prove: $G = C_7 \times C_{29}$.
$K \leq G$, $|K| = 29$, by Cauchy's theorem we have $H \lhd G$, $|H| = 7$.
$K \lhd G$ since $|G : K| = 7$, smallest prime. Then $G = H \times K$. □

Example 1.23.6
$G = D_{4n} = \langle r, s \rangle$, $|r| = 2n$.
Let $H = \langle r^2, s \rangle = D_{2n}$. Then $\varphi : G \to \mathrm{Aut}(H)$ induces a map $G/C_G(H) \to \mathrm{Aut}(H)$.

$C_G(H) = \{1, r^n\} \subseteq G$
$\implies D_{4n}/\langle r^n \rangle \cong D_{2n}$ is isomorphic o a subgroup of $\mathrm{Aut}(D_{2n})$.

$|\mathrm{Aut}(D_{2n})| = \phi(n)n$, $(n \geq 3)$.
For $n = 4$, $D_8 \cong |\mathrm{Aut}(D_8)|$.

Definition 1.23.7

- If $|G| = p^\alpha$ $(\alpha > 0, p$ prime), then G is a p-group
- If $H \leq G$, $|H| = p^\alpha$, then H is a p-subgroup
- $|G| = p^\alpha m$, $(p \nmid m)$, if $H \leq G$, $|H| = p^\alpha$, H is a Sylow p-subgroup
- $\mathrm{Syl}_p(G) = \{\text{Sylow } p\text{-subgroups}\}$, $n_p := |\mathrm{Syl}_p(G)|$.

1.24 Sylow's Theorems

Theorem 1.24.1 Sylow 1
p prime, $|G| = p^\alpha m$ $(p \nmid m, \alpha > 0)$. Then $\mathrm{Syl}_p(G) \neq \emptyset$, $(\exists H \leq, |H| = p^\alpha)$.

Theorem 1.24.2 Sylow 2

(i) Any two Sylow p-subgroups are conjugate

(ii) Any p-subgroup of G is contained in a Sylow p-subgroup

Theorem 1.24.3 Sylow3

(i) $n_p \equiv 1 (\mod p)$

(ii) $n_p | m$

(iii) $n_p = |G : N_G(P)|$ for any $P \in \mathrm{Syl}_p(G)$

Corollary 1.24.4
If $P \in \mathrm{Syl}_p(G)$, then $P \lhd G \iff n_p = 1$. (Follows from 1.24.3 (iii))
(Thm 1.24.3 (ii) and $|G : N_G(P)| = \#$ conjugates of $P \implies$ Thm 1.24.3 (iii))

Example 1.24.5
G finite group, $|G| = p_1^{n_1} \cdots p_k^{n_k}$.
If $n_{p_i} = 1$ for all i, then G is the internal direct product of its Sylow p_i-subgroups.

Example 1.24.6
Groups of order pq, p, q distinct primes, $p < q$.
Theorem $\implies$ $n_p \equiv 1$ (mod p) and n_p divides $q \implies n_p = 1$ or q
$n_q \equiv 1$ (mod q) and n_q divides $p \implies n_q = 1$

If $n_p = 1$, $G \cong C_p \times C_q \cong C_{pq}$.
$n_p = q$: $n_p \equiv 1 \pmod{p} \iff p \big| q-1$.

If $p \nmid q-1$, $\nexists$ non-cyclic group G with $|G| = pq$ if $p \nmid q-1$. (exercise: $|G| = 15 \implies G$ cyclic)

Assume $n_p = q$, $p \big| q-1$. Let $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$. Then $Q \lhd G$ and $P \not\lhd G$ since $n_p = 1 \iff P \lhd G$.
Exercise: $G = PQ$, $P \cap Q = \{1\} \implies G \cong Q \rtimes_\varphi P$ for some $\varphi : P \to \mathrm{Aut}(Q)$ non-trivial.

$\varphi : C_p \to \mathrm{Aut}(C_q) \cong C_{q-1}$.
φ-nontrivial $\implies \varphi$ injective. Since $p \big| q-1$, $\varphi(C_p)$ is the unique subgroup of order p in C_{q-1}.
$\implies Q \rtimes_{\varphi_1} P = Q \rtimes_{\varphi_2} P$, where φ_1, φ_2 nontrivial.

Lemma 1.24.7
$|G| = p^n m$, $Q :=$ p-subgroup of G, $P \in \mathrm{Syl}_p(G)$, then $N_G(P) \cap Q = P \cap Q$.

Proof
Later. □

Proof of Sylow 3(ii)
$P \subseteq N_G(P) \subseteq G \implies |G : N_G(P)| \Big| |G : P|$. □

Proof of Sylow 1
Remark: if $\alpha = 0$, then theorem holds.
Induction on $|G|$. Assume $|G| > 1$. Fix a prime p, $|G| = p^\alpha m$, $\alpha > 0$. Assume $\mathrm{Syl}_p(G) \neq \emptyset \quad \forall G'$, $|G'| < |G|$.

Case I: $p \big| |Z(G)|$.

By Cauchy's theorem for abelian groups, $\exists H \leq Z(G)$, $|H| = p$. $H \lhd G \implies$ apply induction to G/H: $|G/H| p^{\alpha-1} m$.
$\implies \exists \overline{K} \leq G/H$, $|\overline{K}| = p^{\alpha-1}$. Then $\overline{K} = K/H$ for some $H \subseteq K \subseteq G$. Then $|K| = |\overline{K}||H| = p^\alpha$.

Case II: $p \nmid |Z(G)|$.

By the class equation:
$$|G| = |Z(G)| = \sum |G : C_g(y)$$
where the summation is over y as conjugacy class rep for classes with > 1 element.
$\implies \exists y$ such that $p \nmid |G : C_g(y)|$. So $|C_G(y)| = p^\alpha k$ $(k < m)$.
By induction, $|H| = p^\alpha$, $H \leq C_g(y)$. □

Proof of Sylow 2, 3(i)
G acts on {subgroups of G of order l} by conjugation. In particular, G acts on $\mathrm{Syl}_p(G)$.

Fix $P \in \mathrm{Syl}_p(G)$. (By Sylow 1, $\exists$ at least one)
Set
$$\mathcal{J} := \{P_1, \ldots, P_r\} \qquad \text{all disjoint conjugates of } P.$$
G acts on $\mathcal{J}$ transitively. If $Q \leq G$, Q acts on $\mathcal{J}$, say. (Q arbitary).

$$\mathcal{O}_1 = \{P_1, \ldots\}, \mathcal{O}_2 = \{P_2, \ldots\}, \ldots, \mathcal{O}_s = \{P_s, \ldots\} \qquad 1 \leq s \leq r$$

Then:

- $r = |\mathcal{J}| = \sum_{i=1}^{s} |\,\mathcal{O}_i\,|$
- $|\,\mathcal{O}_i\,| = |Q_{P_i}|$
- $Q_{P_i} = \{x \in Q \mid xP_ix^{-1} = P_i\} = N_G(P_i) \cap Q$

Then if $Q = P_1$, lemma $\implies Q_{P_i} = P_i \cap Q$.

$\implies r = \sum_{i=1}^{s} |P_1 : P_1 \cap P_i|$. $\begin{matrix} \text{If } P_i = P_1 \implies |P_1 : P_1| = 1 \\ \text{If } P_i \neq P_1 \implies p \big| |P_1 : P_i \cap P_1| \end{matrix}$.

$\implies r \equiv 1 \bmod p$.

If $Q = p$-subgroup of G,

Claim: $Q \subseteq P_i$ for some i.

Proof of Claim:
(Claim $\implies \mathcal{J} = \mathrm{Syl}_p(G)$, $P' \subseteq P_i \implies r = n_p \implies n_p \equiv 1 \bmod p$)
$r = \sum_{i=1}^{s} |Q : P_i \cap Q|$.
Assume $Q \not\subseteq P_i$ for all i. Then $P_i \cap Q \neq Q$, so

$$|Q : P_i \cap Q| = 1 \implies P \big| |Q : P_i \cap Q| \quad \forall i \implies p \big| r$$

Contradiction. ■

□

Remark: $H, K \leq G$. $H \subseteq N_G(K) \implies$

- $HK \leq G$
- $K \lhd HK$ and $H \cap H \lhd H$ and $HK/K \subseteq H/K \cap H$.

Proof of Lemma 1.24.7
Let $H = N_G(P) \cap Q$. Want to show $H \subseteq P \cap Q$.
Clearly, $H \subseteq Q$. We will show that $P = PH$. ($\implies H \subseteq PH = P$)
Enough to prove that PH is a p-subgroup.
Remark $\implies |PH| = \frac{|P||H|}{|P \cap H|}$ (all p-subgroups). □

Example 1.24.8
Groups of order 30: $30 = 2 \cdot 3 \cdot 5$
$n_5 \equiv 1$ (mod 5), $n_5 \big| 6 \implies n_5 = 1$ or 6.
$n_3 \equiv 1$ (mod 3), $n_3 \big| 10 \implies n_3 = 1$ or 10.

If $n_5 = 6$ and $n_3 = 10$, then: $\begin{matrix} 24 & \text{elements of order 5} \\ 20 & \text{elements of order 3} \end{matrix}$, cannot happen!

Let $P \in \mathrm{Syl}_5$, $Q \in \mathrm{Syl}_3$. Either $P \lhd G$ or $Q \lhd G$.
Let $H := PQ$, so $H \leq G$, $|H| = 15 \implies H = C_{15}$, $H \lhd G$. G has element of order 2 $\implies G \cong H \rtimes_\varphi C_2$, $\varphi : C_2 \to \mathrm{Aut}(C_{15}) = C_2 \times C_4$.

$\implies$ 4 such homomorphisms:
Have 4 non-isomorphic groups of order 30: $C_{30}, D_{30}, C_5 \times S_3, C_3 \times D_{10}$.

	n_3	n_5	n_2
C_{30}	1	1	1
D_{30}	1	1	15
$C_5 \times C_3$	1	1	3
$C_3 \times D_{10}$	1	1	5

1.25 Applications of Sylow's Theorem

General Situation
$H \leq G$, $k = |G : N_G(H)| = \#$ conjugates, $H_1, \ldots H_k$, of H.
Recall: $G \xrightarrow{\varphi} S_k$ has $\ker(\varphi) = \bigcap_{i=1}^{k} N_G(H_i)$.
Remark: If G simple, $k > 1$, $(H \not\lhd G) \implies \ker(\varphi) = \{1\}$.

$$\implies \qquad G \hookrightarrow S_k \implies |G|/k!$$

So if $H \in \mathrm{Syl}_p(G)$, then $k = n_p$.

Example 1.25.1 (Groups of order 12)
Sylow's Theorem $\implies n_3 = 1$ or 4, $n_4 = 1$ or 3. Let $P \in \mathrm{Syl}_3$, $Q \in \mathrm{Syl}_2$.

Assume $P \not\lhd G$ $(n_3 = 4)$
G acts on $\mathrm{Syl}_3 = \{P_1, \ldots, P_4\}$, $|P_i| = 3$
$\implies G \xrightarrow{\varphi} S_4$, $\ker(\varphi) = \bigcap_{i=1}^{4} N_G(P_i)$
$4 = n_3 = |G : N_G(P_i)| \implies |N_G(P_i)| = 3 \implies N_G(P_i) = P_i$
$\implies \ker(\varphi) = \bigcap_{i=1}^{4} P_i = \{1\}$, ($P_i$'s distinct, order 3).
$\implies G \leq S_4$, $n_3 = 4 \implies$ 8 elements of order 3.

Elements of order 3 in S_4: (ijk), $(\# = 8)$
$\implies$ all 3-cycles in S_4 are in G.
$\implies A_4 \subseteq G$ ($A_4 =$ generates by 3-cycles)
$|G| = |A_4| = 12 \implies G = A_4$.

Case: $P \lhd G$ $(n_3 = 1)$
$P \lhd G$, $|P| = 3$, $Q \in \mathrm{Syl}_2$, $|Q| = 4$.
$\implies G \cong P \rtimes_\varphi Q$, $\varphi : Q \to \mathrm{Aut}(P) \cong C_2$, $(P \cong C_3)$.
$Q \lhd G \iff \varphi =$ trivial.
If $n_2 = 1$, $(Q \lhd G)$: $G \cong P \times Q$, have $G \cong C_3 \times C_4$ or $G \cong C_3 \times C_2 \times C_2$.

Assume $Q \not\lhd G$ $(n_2 = 3)$: $\varphi \neq$ trivial.

Case $Q \cong C_4$: $\exists! \varphi : C_4 \to C_2$ non-trivial
$\varphi(\widehat{1}) = \widehat{1}$, $C_2 \cong \mathrm{Aut}(C_3) = \{Id, x \mapsto -x\}$
$\implies G \cong C_3 \rtimes_\varphi C_4$ - Dicyclic group of order 12.

Case $Q \cong C_2 \times C_2$: $\exists 3$ $\varphi : C_2 \times C_2 \to C_2$ non-trivial
$\implies$ isomorphic $C_3 \rtimes_\varphi (C_2 \times C_2)$ since the image of $\varphi = C_2$

Claim: $G \cong C_2 \cong C_2 \times S_3$
- $\exists$ normal subgroup of order 3
- $\nexists$ element of order 4

Example 1.25.2
$|G| = 60$, G simple $\implies G \cong A_5$.

Proof
G simple $\implies n_p \neq 1$ $\forall p = 2, 3, 5$
$n_2 \neq 1, n_2 \big| 15 \implies n_2 = 3, 5$ or 15.

$n_5 \neq 1$, $n_5 \equiv 1(\bmod 5)$, $n_5 \big| 6 \implies n_5 = 6$.
G acts on $\mathrm{Syl}_p \implies G \xrightarrow{\varphi} S_{n_p}$
$n_p \neq 1$, G simple $\implies G \overset{\varphi}{\hookrightarrow} S_{n_p}$
$\implies n_2 \neq 3$, $|G| = 60 > |S_3|$.

Case $n_2 = 5$: $G \overset{\varphi}{\hookrightarrow} S_5$
$|G| = 60$, $G \leq S_5 \implies |S_5 : G| = 2 \implies G \lhd S_5$
$\implies G = A_5$.

This actually happens: $\exists$ 5 subgroups of order 4 (and not 15). All these subgroups are not cyclic, elements of order 2 in A_5 looks like $(ij)(kl)$ and there are 15 of them. $\implies n_2 \neq 15$.

Case $n_2 = 15$: If any $P, Q \in \mathrm{Syl}_2$ $(P \neq Q)$ have $P \cap Q = \{1\}$, then $\exists 15 \cdot 3 = 45$ elements of order 2 or 4

$n_5 = 6 \implies 6 \cdot 4 = 24$ elements of order 5
$\implies 45 + 24 > 60$
$\implies \exists P, Q \in \mathrm{Syl}_2$, $|P \cap Q| = 2$ $(|P| = |Q| = 4)$

Let $N = N_G(P \cap Q)$: $P, Q \subseteq N, P \neq Q \implies 4 \big| |N|, |N| > 4$. $|N| \big| 60 \implies |N| = 12$, 20 or 60.

Case $|N| = 60$: $N = G \implies P \cap Q \lhd G$. Contradiction, G is simple.

Case $|N| = 20$: $|G : N| = 3 \implies$ # conjugates of N is 3, N_1, N_2, N_3. G acts on $\{N_1, N_2, N_3\}$.
$\implies G \to S_3$ non-trivial $\implies \ker \varphi = G, \{1\}$. Contradiction.

Case $|N| = 12$ $|G : N| = 5 \implies \exists 5$ conjugates for N, $N_1, \ldots, N_5$.
$\implies G \xrightarrow{\varphi} S_5$ non-trivial $\implies \ker \varphi = \{1\} \implies G \cong A_5$, $|S_5 : G| = 2$. This case does not occur. $\square$

1.26 Simple Groups of Order ≤ 200

Find all $n \leq 200$ such that $\exists G$, $|G| = n$, G simple. $(n \neq p$ prime$)$
Remark: $|G| < \infty$, G abelian. G simple $\iff G \cong C_p$, p prime.

Step 0: Sylow's Theorem. If $n_p = 1$ then G is not simple:
$|G| = p^\alpha m$, $p \nmid m, m > 1$ - all $P \in \mathrm{Syl}_p$ is normal $|G| = p^\alpha$, $\alpha > 1$ - $Z(G) \neq \{1\}$, $Z(G) \lhd G \implies G$ not simple
This rules out everything except 12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96, 105, 108, 112, 120, 132, 144, 150, 160, 168, 180, 192.

For example: $189 = 9 \cdot 21 = 27 \cdot 7$
$n_7 \big| 27, n_7 \equiv 1(\bmod 7) \implies n_7 = 1$.

Step 1 If G acts on X of size n in a nontrivial way, then $f : G \to S_n$ nontrivial map.
$\ker f \lhd G$ and $\ker f = \{1\}$, i.e. f injective $\implies |G|$ divides $n!$.

In particular, if $X = \mathrm{Syl}_p(G)$, $|X| = n_p$, $|G| \big| n_p!$ for all $p \big| |G|$.

Example 1.26.1
$|G| = 72 = 2^3 \cdot 3^2$, $n_3 \big| 8$, $n_3 \equiv 1 \ (\bmod 3) \implies n_3 = 4$, but $72 \nmid 4!$.

$|G| = 192 = 2^8 \cdot 3$, $n_2 \big| 3$, $n_2 \equiv 1 \ (\bmod 2) \implies n_2 = 3$, $192 \nmid 3!$.

Remark: May apply same argument for all $f : G \to S_n$.

- G acts on $\{\text{conjugates of } H\}$, $H \not\trianglelefteq G \implies G \xrightarrow{f} S_n$, $n = |G : N_G(H)| > 1$.
  G simple $\implies$ f injective.
- G acts on $G/H = \{\text{left cosets}\}$, $H \lneq G$
  $\implies \varphi : G \to S_{G/H} \cong S_n$, $n = |G : H|$.
  $\ker\varphi$ is the largest normal subgroup of G contained in $H \implies \ker\varphi = \{1\} \implies \varphi$ injective.

Refinement of Step 1: If $n \geq 5$, $|G| > 2$, $G \hookrightarrow S_n$. G simple $\implies G \hookrightarrow A_n$.

Proof
Otherwise, $G \cap A_n \lhd G$ so $xyx^{-1} \in G \cap A_n$.
G simple $\implies G \cap A_n = G$ or $\{1\}$, $G \not\subseteq A_n \implies G \cap A_n = \{1\}$. Bu then $G \to S_n \to S_n/A_n \cong C_2$ and $G \hookrightarrow C_2$ but $|G| > 2$. □

Example 1.26.2
$|G| = 112 = 16 \cdot 7 \implies n_2 \big| 7 \implies n_2 = 7$.
Then $|G|$ divides $7!$ but $|G| \nmid \frac{7!}{2} = |A_n|$.

Refinement 2: If G is simple, $G \hookrightarrow S_n$, $(n \geq 5)$, then $G \in A_n$ (and $|G| \big| \frac{n!}{2}$) and either

$$G \cong A_n \quad \text{or} \quad |A_n : G| \geq n \qquad (\text{so } |G| \leq \frac{(n-1)!}{2})$$

Remark: $n \geq 5$, any proper $H \leq A_n$ has index $|A_n : H| \geq n$.

Proof
Consider $\varphi : A_n \to S_n$, $l = |A_n : H|$ (left multiplication on cosets of H).
$\ker\varphi :=$ largest subgroup of A_n contained in $H \implies \ker\varphi = \{1\}$, $n \geq 5$.

$$A_n \hookrightarrow S_l \implies \frac{n!}{2} \geq l! \implies l \geq n$$

□

Example 1.26.3
$|G| = 90 = 2 \cdot 3^2 \cdot 5$, $n_5 \big| 18$, $n_5 \equiv 1 \pmod 5 \implies n_5 = 6$.
Now, $90 \big| \frac{6!}{2} \implies G \neq A_6$, $90 \neq \frac{(6-1)!}{2} = 3 \cdot 4 \cdot 5 = 60$. Contradiction.

Step 2(Element Counting)
If for smallest value of $n_p > 1$ satisfying Sylow, we have

$$\sum n_p(p-1) + 1 > |G|$$

Contradiction.

Example 1.26.4
$n = 105 \implies 3 \cdot 5 \cdot 7 \implies n_7 = 15, n_5 = 21, n_3 = 7$.
$15 \cdot 6 + 21 \cdot 4 + 7 \cdot 2 + 1 = 90 + 84 + 12 > 105$.

Refinement (Count overlaps)

Example 1.26.5
$|G| = 56 = 7 \cdot 2^3 \implies n_7 = 8, n_2 = 7 \implies 8 \cdot 6 + 7 + 1 = 56$.
$7 + 1 = |P|$, $P \in \mathrm{Syl}_2$ but $n_2 > 1$ so there must be some $Q \in \mathrm{Syl}_2$, $P \neq Q$, so $|P \cap Q| \leq 4$. (Same for 132)

Step 3 Construct H, with small $|G : H|$.
For example, $H = N_G(P \cap Q)$, $P, Q \in \mathrm{Syl}_p$, $P \neq Q$.

Example 1.26.6
$|G| = 144 = 2^4 \cdot 3^2$, $n_3 | 16 \implies n_3 = 4$ or 16, but $144 \nmid 4! \implies n_3 = 16$.

If $P \cap Q = \{1\}$, for all $P \neq Q$ in Syl_3, then $16 \cdot (9-1) + 16 \neq 144$, $16 = \mathrm{Syl}_2$. $\implies n_2 = 1 \implies |P \cap Q| = 3$.

Let $H = N_G(P \cap Q)$, since $P \cap Q \lhd P$ (index 3), $P \cap Q \lhd Q \implies P, Q \subset H$.
So $|H| > 9 \implies |H| = 18, 36, 72, 144$.

- $|H| = 144 \implies |H| = |G| \implies P \cap Q \lhd G$
- $|H| = 72 \implies |G : H| = 2 \implies H \lhd G$
- $|H| = 18 \implies P, Q \lhd H$ (index 2) $\implies P, Q \in \mathrm{Syl}_3(H)$, contradiction
- $|H| = 36 \implies |G : H| = 4$, but $|G| \nmid 4!$ $(\varphi : G \hookrightarrow S_4 = S_{G/H})$

Exercise: $n = 180$.

For $n = 168$, $G = GL_3(\mathbb{F}_2)$.

$$|G| = \underbrace{(2^3 - 1)}_{\substack{\text{choice for} \\ \text{row 1}}} \underbrace{(2^3 - 2)}_{\substack{\text{choice for} \\ \text{row 2}}} (2^3 - 2 \cdot 2) = 7 \cdot 6 \cdot 4 = 168$$

Exercise: $|GL_n(\mathbb{F}_p)| = ?$

1.27 Nilpotent and Solvable Groups

Definition 1.27.1
Let G be a group. The upper central series of G is the chain of subgroups of G

$$\{1\} = Z_0(G) \subseteq Z_1(G) \subseteq \dots$$

defined as $Z_1(G) = Z(G) = Z(G/Z_0(G))$,

$$Z_{i+1}(G) \leq G \quad \text{such that} \quad Z_{i+1}(G)/Z_i(G) \cong Z(G/Z_i(G)).$$

(Z_{i+1} is the pre-image of the centre)
Remark:

(i) All $Z_i(G) \lhd G$

(ii) If $Z(G) = \{1\}$, then all $Z_i(G) = 1$

(iii) If $Z_k(G) = G$ for some k, then $Z_i(G) = G$ for all $i \geq k$

Example 1.27.2
$G = Q_8$, then $Z_1(G) = \{\pm 1\}$, $Z_2(G) = Z(Q/\{\pm 1\}) = Q_8$.

Definition 1.27.3
If $Z_c(G) = G$ for some c, then G is nilpotent and that smallest such c is the nilpotency class of G.
Remark:

- Abelian groups are nilpotent
- G nilpotent with class $c \iff G/Z(G)$ nilpotent with class $c-1$
- D_{2k} nilpotent $\iff k = 2^l$ for some l

Example 1.27.4
D_{2^n} is nilpotent with class $n-1$.

Proof
Induction n, $Z(D_{2^{n+1}}) = \{1, r^{2^{n+1}}\}$

$$D_{2^{n+1}}/Z(D_{2^{n+1}}) \cong D_{2\cdot 2^n} = D_{2^n}$$

□

Theorem 1.27.5
G finite, $|G| = p_1^{n_1} \cdots p_k^{n_k}$. Let $P_i \in \mathrm{Syl}_{p^i}(G)\ \forall i = 1, \ldots, k$. Then G nilpotent $\iff G \cong P_1 \times \cdots \times P_k$.
$(\iff n_{p^i} = 1\ \ \forall i)$

Proposition 1.27.6
If G is a p-group, $|G| = p^a$, then G is nilpotent of class $\leq a-1$.

Proof
Induction on a. $|G| = p$ abelian $\implies$ nilpotent.
Suppose true for all $a < k$.
Then if $|G| = p^k$, it has a non-trivial centre, $|Z(G)| \geq p$ and $|G/Z(a)| = p^a$ where $a < k$. By induction, $G/Z(G)$ is nilpotent of class $\leq a-1$, so G is nilpotent of class $\leq a \leq k-1$ by remark (ii). □

Proof of Theorem
Follows from proposition. □

Lemma 1.27.7
If $P \in \mathrm{Syl}_p(G)$, then $PZ(G)/Z(G) \in \mathrm{Syl}_p(G/Z(G))$ and $P \cap Z(G) \in \mathrm{Syl}_p(Z(G))$. In particular, $P, Q \in \mathrm{Syl}_p(G) \implies P \cap Z(G) = Q \cap Z(G)$ since $|\mathrm{Syl}_p(Z(G))| = 1$.

Proof
Suppose $p^a \big| |G|$ and $p^{a+1} \nmid |G|$ $\quad (p^a \big| |G|)$ and $p^b \big| |G|$. Now,

$$PZ(G)/Z(G) \cong P/P \cap Z(G) \qquad \text{(2nd iso. thm)}$$

$$|P \cap Z(G)| \leq p^b \implies |P/P \cap Z(G)| \geq p^{a-b} \quad \text{with equality} \quad \iff |P \cap Z(G)| = p^b$$

$|PZ(G)/Z(G)|$ is a p-group in $G/Z(G)$, $p^{a-b} \big| |G/Z(G)|$.
So $|PZ(G)/Z(G)| \leq p^{a-b} \implies |P/P \cap Z(G)| = p^{a-b}$

$$\implies P \cap Z(G) \in \mathrm{Syl}_p(Z(G)) \quad \text{and} \quad PZ(G)/Z(G) \in \mathrm{Syl}_p(G/Z(G)).$$

□

Proof of Theorem
Recall that if $H, K \lhd G$ and $H \cap K = \{1\}$, then elements of H and K commute.

Then we've reduced to showing that each $P_i \lhd G$. (If $i \neq j$, $P_i \cap P_j$, so $P_1, \ldots, P_k$ commuter preserve)

$$P_1 \times \cdots \times P_k \to G \quad \text{by} \quad (x_1, \ldots, x_n) \mapsto (x_1 \cdots x_n)$$

To show $n_p = 1$, induct on $|G|$. Suppose $P, Q \in \mathrm{Syl}_p(G)$.
$\implies PZ(G)/Z(G)$, $QZ(G)/Z(G)$ are p-subgroups of $G/Z(G)$.
($|G/Z(G)| < |G|$ so G nilpotent)
So by induction $PZ(G)/Z(G) = QZ(G)/Z(G) \implies PZ(G) = QZ(G)$.

$P, Q \leq H \leq G \implies P, Q \in \mathrm{Syl}_p(H)$, but $P \lhd PZ(G) = H$.
$\implies |\mathrm{Syl}_p(H)| = 1 \implies P = Q$. □

Definition 1.27.8
A composition series for a finite group G is a series of subgroups

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

such that G_{i+1}/G_i are all simple.

Theorem 1.27.9
Any finite group has a composition series.

Proof
Induction on $|G|$.
Base Case: If G is simple, then $\{1\} \lhd G$ is a composition series.
Induction: Suppose G is not simple $\implies \exists$ nontrivial normal subgroup $H \lhd G \implies |H| < |G| \implies H$ has a composition series

$$\{1\} = H_0 \lhd \cdots \lhd = H$$

But also, $|G/H| < |G|$, G/H has a composition series

$$\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_l = G/H/$$

$\implies \exists! G_i \supset H \ni G_i/H = K_i. \qquad (G_0 = H,\ G_l = G).$

Then $H = G_0 \lhd G_1 \lhd \cdots \lhd G_l = G. \qquad (G_{i+1}/G_i \cong (G_{i+1}/H)/G_i/H$ is simple).

So

$$\{1\} = H_0 \lhd \cdots \lhd H \lhd G_1 \lhd \cdots \lhd G_l = G$$

is a composition series for G. □

Remark: In fact, if $H \lhd G$, $\exists$ a composition series containing H. Moreover, if $1 \lhd H_1 \lhd \cdots \lhd H_n \lhd G$, then there is a composition series containing all H_i (a refinement).

Theorem 1.27.10 (Jordan-Hölder)
Suppose $\{1\} = G_0 \lhd \cdots \lhd G_n = G$ and $\{1\} \lhd H_0 \lhd \cdots \lhd H_m = G$ are two composition series for G. Then $m = n$, and $\{G_{k+1}/G_k\} = \{H_{k+1}/H_k\}$ up to isomorphism.

Example 1.27.11
If K, K' simple, then

$$\{1\} \lhd K \times \{1\} \lhd K \times K' \quad \text{and} \quad \{1\} \lhd \{1\} \times K' \lhd K \times K'.$$

Proof
See book for complete proof.
Hint: Consider a simple group H_1.

$$\{1\} \lhd G_1 \cap H_1 \lhd G_2 \cap H_2 \lhd \cdots \lhd G_n \cap H_n = H_1$$

$\implies \exists k$ such that $\begin{matrix} G_i \cap H_1 = H_1 & \forall i \geq k \\ G_i \cap H_i = \{1\} & \forall i < 0 \end{matrix}$. So

$$H_1 \cong G_{i+1} \cap H_1 / G_i \cap H_1 \to G_{i+1}/G_i \quad \text{simple.}$$

□

Definition 1.27.12
G is <u>solvable</u> if all of its quotients G_{i+1}/G_i in a composition series for G are cyclic. (prime order)
($\iff \exists 1 \lhd H_1 \lhd \cdots \lhd H_n = G$ such that H_{i+1}/H_i is abelian.)
<u>Remark</u>: Thus, nilpotent groups are solvable since $\{1\} = Z_0 \lhd Z_1 \lhd \cdots \lhd Z_n = G$ and $Z_{i+1}/Z_i = Z(G/Z_i)$ is abelian.
The reverse is not true: S_4 is solvable but not nilpotent.

Recall: $G' :=$ commutator subgroup of G, $G^{(n)} = (G^{(n+1)})'$.

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots$$

Theorem 1.27.13
G solvable $\iff G^{(n)} = \{1\}$ for some n.

Proof
($\Leftarrow$) $G^{(i)}/G^{(i+1)}$ is abelian.
($\Rightarrow$) Suppose $\{1\} \lhd G_0 \lhd \cdots \lhd G_m = G$ solvable, then G_m/G_{m-1} is abelian $\implies G^{(i) \leq G_{m-1}}$. By induction, $G^{(i)} \leq G_{m-i}$. □

Corollary 1.27.14
If $H \leq G$, G solvable $\implies H$ is solvable.

Proof
$H^{(i)} < G^{(i)}$. □

{Cyclic Groups}$\subsetneq$ {Abelian Groups}$\subsetneq$ {Nilpotent Groups}$\subsetneq$ {Solvable Groups}

$\exists$ nilpotent groups that are not abelian: p-groups, D_{2n}
G nilpotent $\implies G$ solvable

$$\{1\} = Z_0(G) \subseteq Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots \subseteq Z_n(G) = G$$

$$\text{(abelian)} \qquad Z_{i+1}(G)/Z + i(G) = Z(G/Z_1(G)) = G/Z_1(G)$$

$\implies \{1\} \lhd Z_1 \lhd Z_2 \lhd \cdots \lhd Z_n = G$, Z_{i+1}/Z_i abelian for each i.
$\implies G$ solvable.

$\exists$ solvable groups that are not nilpotent: $D_{2k}, k \neq 2^n$.
$\{1\} \lhd \langle r \rangle \lhd D_{2k}$.

S_n is not solvable if $n \geq 5$.
$\{1\} \lhd A_n \lhd S_n$, A_n is the only non-trivial normal subgroup.

Theorem 1.27.15 (On Solvable Groups)

(i) Feit-Thompson: $|G|$ odd $\implies$ G solvable

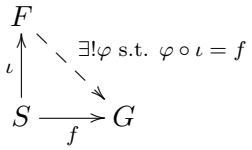
(ii) Burnside: $|G| = p^a \cdot 2^b$, p, q, prime $\implies$ G solvable

(iii) Philip Hall: $|G| = p^a \cdot m$, $p \nmid p$ prime $\implies$ G solvable

(iv) If $\langle x, y \rangle$ solvable $\forall x, y \in G \implies G$ solvable

1.28 Free Groups

Definition 1.28.1
F group, $S \subseteq F$ subset.
F is a free group with basis S if $\forall$ group G and $\forall f : S \to G$, $\exists!$ homomorphism $\varphi : F \to G$ such that $\varphi(x) = f(x) \quad \forall x \in S$.



Existence of Free Groups

Definition 1.28.2
A word on a set S is an expression of the form $e_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ where $e_i = \pm 1$, $x_i \in S \cup \{1\}$. (same as a function $\{1, \ldots, n\} \to S \cup S_{-1} \cup \{1\}$).
Reduced word is a word with no obvious cancellations, e.g.: $xyy^{-1}x, x \cdot 1 \cdot y$.
$1 =$ empty word.
Subword of $e_1^{e_1} \cdots x_n^{e_n}$ is $e_r^{e_r} \cdots x_s^{e_s}$ $1 \leq r \leq s \leq 1$.

Definition 1.28.3
$x_1^{e_1} \cdots x_n^{e_n}$ is a reduced word if it is either 1 or

- $x_{i+1} = x_i^{-1}$ $\forall i$
- $x_i \neq 1$ $\forall i$

Definition 1.28.4
Two words are equivalent if one can be obtained from the other by successively adding or deleting subwords of the form $xx^{-1}, x^{-1}, 1$.
$\exists!$ reduced word in every equivalence class.

$yxzz^{-1}x^{-1}y^{-1}yx \to yxx^{-1}y^{-1}yx \to yy^{-1}yx \to yx$
$yxzz^{-1}x^{-1}x \to yxzz^{-1} \to yx$

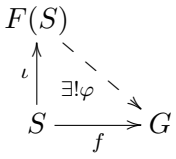
Definition 1.28.5
$F(S) =$ set of equivalence classes of words on S.
Multiplication $=$ juxta position of words.

Example 1.28.6
$(xxyx, x^{-1}xyzx) \mapsto xxyyxx^{-1}yzx$

"1" = empty word 1.

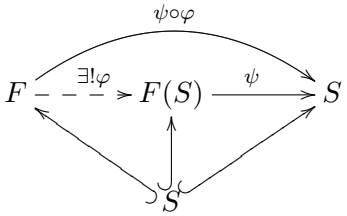
Claim: $F(S)$ is a free group woth basis S.
Exercise: $F(S)$ is a group.
$(x_1^{e_1} \cdots x_n^{e_n})^{-1} = x_n^{-e_n} \cdots x_1^{-e_1}$.
Remark: $|S| > 1$, $F(S)$ is non-abelian.
$x, y \in S$, $xy \neq yx$. $S = \{x_1, \ldots, x_n\}$, $\{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}, 1\}$.

$S \overset{\iota}{\hookrightarrow} F(S)$, $x \mapsto x$

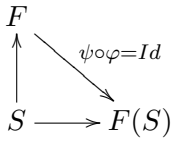


$\varphi(x_1^{e_1} \cdots x_n^{e_n} = f(x_1)^{e_1} \cdots f(x_n)^{e_n})$

Remark: A free group F with basis S is unique up to isomorphism, i.e. $F \cong F(S)$.



$\implies \psi \circ \varphi = Id$ is the unique isomorphism $F \to F$ such that



$\implies \psi \circ \varphi = Id$ is the unique homomorphism $F \to F$ satisfying the diagrams $\implies \varphi \circ \psi = Id_{F(S)}$.

$F(S)$ = free goup on the set S. $|S|$ = rank of $F(S)$.

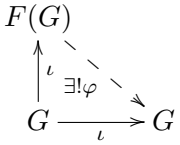
Notation: $x^m y^n = x \cdots x y \cdots y$, m and n times respectively for positive $m, n \in \mathbb{Z}$.

Theorem 1.28.7
Subgroups of free groups are free.
Exercise: Free groups of rank 2 have a subgroup that is infinitely generated.

1.29 Presentations of a Group

G group, $\exists!$ surjective homomorphism.

$$\varphi : F(G) \twoheadrightarrow G \quad \text{such that} \quad \varphi(\underbrace{x_1^{e_1} \cdots x_n^{e_n}}_{\text{word on } G}) = \underbrace{x_1^{e_1} \cdots x_n^{e_n}}_{\text{product in } G} \qquad \forall x_1, \ldots, x_n \in G$$



such that $\varphi(x) = x \quad \forall x \in G$ (LHS word, RHS in G)

If $S \subseteq G$ subset, then $G = \langle S \rangle \iff \exists$ surjective hom $\varphi : F(S) \to G$ s.t. $\varphi(x_1^{e_1} \cdots x_n^{e_n})$ $\forall x_1 \cdots x_n \in S$.

Definition 1.29.1
A presentation for a group G is a $\langle S \mid R \rangle$ where S = generating set and R = relations. Formally, S = set of elements in G, R = set of words in $F(S)$.

To give presentations, we need:
1. $G = \langle S \rangle \implies \varphi : F(S) \twoheadrightarrow G$
2. $\ker \varphi$ = smallest normal subgroup of $F(S)$ that contains R

In general, $H \leq G$, then

$$\text{the smallest normal subgroup of } G \text{ containing } H = \langle \bigcup_{x \in G} (xHx^{-1}) \rangle$$

$\forall K \lhd G$, $H \subseteq K \implies N \subseteq K$.

Warning: $\ker \varphi \not\supseteq \langle R \rangle$
e.g. if $a^2 \in R$, then $a^2 = 1$ in $G \implies xa^2x^{-1} = 1$ in G.
2. $\implies F(S)/N \cong G$

Definition 1.29.2
G is finitely generated f G has a presentation $G = \langle S \mid R \rangle$ where S is finite.
G is finitely presented if G has a presentation $G = \langle S \mid R \rangle$ where S, R are finite.

Notation for relations: $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^[-1] \rangle$, $R = \{r^n, s^2, srsr\}/$
Remark: A group can have different presentations:

$$\begin{aligned} S_3 \cong D_6 &= \langle r, s \mid r^3 = s^2 = 1, rs = sr^2 \rangle \\ &= \langle a, b \mid a^2 = b^2 = (ab)^3 = 1 \rangle \end{aligned}$$

$a = (1\ 2)$, $b = (1\ 3)$.

For any G such that $G = \langle a, b \rangle$ with $a^2 = 1, b^2 = 1, (ab)^3 = 1$ then $G = \{1, a, b, ab(= baba), ba(= abab), aba(= bab)\}$

Example 1.29.3
Any finite G is finitely presented.

Criterion
$|G| = n < \infty$ then $G = \langle S, R \rangle$ if

(i) $\langle S \rangle = G$

(ii) Any group generated by elements in S with relations given by R has $\leq n$ elements.

Example 1.29.4
$G = \{x_1, \ldots, x_n\}$, let $S = G$

$$\varphi : F(G) \twoheadrightarrow G, \varphi(x_i) = x_i \quad \forall i$$

Let $R =$ set of words $x_i x_j x_k^{-1}$ for all $x_i x_j = x_k$.
Then $R \subseteq \ker \varphi$. Let $N =$ normal subgroup generated by $R \implies N \subseteq \ker \varphi$.

$$\begin{array}{ccc} F(G) & \xrightarrow{\varphi} & G \\ \downarrow & \nearrow_{\overline{\varphi}} & \\ F(G)/N & & \end{array}$$

$\overline{\varphi}$ is an isomomorphism: show that $|F(G)/N| = n$.

Claim: $F(G)/N = \{\widehat{x_1}, \ldots, \widehat{x_n}\}$, $\widehat{x_i}$ coset of x_i.
$\supseteq$ is clear.
$\{\widehat{x_1}, \ldots, \widehat{x_n}\}$ closed under multiplication
$\widehat{x_i}\widehat{x_j} = \widehat{x_k}$ if $x_i x_j = x_k \iff \widehat{x_i x_j x_k^{-1}} = \widehat{1}, x_i x_j x_k^{-1} \in R$

Presentation: $G = \langle S, R \rangle$.
Generators: $S \subseteq G$, $\langle S \rangle = G \implies F(S) \xrightarrow{\varphi} G$. $S \hookrightarrow F(S), G$.

$$\varphi(\underbrace{s_1^{e_1} \cdots s_n^{e_n}}_{\text{word}}) = \underbrace{s_1^{e_1} \cdots s_1^{e_n}}_{\in S}$$

Relations $R \subseteq F(S)$ such that $\ker \varphi =$ normal subgroup genereated by R.

Recall: $A \subseteq G$
Normal subgroup generated by $A = \langle \bigcup_{x \in G} xAx^{-1} \rangle$
(smallest $H \lhd G, A \subseteq G$)

$$\implies \qquad G \cong F(S) / \langle \bigcup_{x \in F(S)} xRx^{-1} \rangle$$

Criterion
$|G| = m$, then $G = \langle S \mid R \rangle$ if:

(i) $G = \langle S \rangle$

(ii) Elements in S have to satisfy relations in R

(iii) Any group G' with generators $x_1, \ldots, x_n$ satisfying relations in R, then $|G'| \leq m$

Proof
$G = \langle S \rangle \implies F(S) \overset{\varphi}{\twoheadrightarrow}, \varphi(s_1^{e_1} \cdots s_n^{e_n})$.
Let $N =$ normal subgroup in $F(S)$ in $F(S)$ genereated by R.
(ii) $\implies R \subseteq \ker \varphi \implies N \subseteq \ker \varphi$
$\implies \varphi$ factors through $\overline{\varphi}$
$\implies \overline{\varphi}$ surjective

$$\begin{array}{ccc} F(S) & \xrightarrow{\varphi} & G \\ \downarrow & \nearrow_{\overline{\varphi}} & \\ F(S)/N & & \end{array}$$

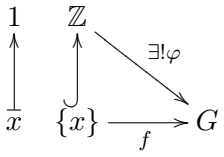
Take $G = F(S)/N = \langle \underbrace{\widehat{s_1}, \ldots, \widehat{s_n}}_{\text{satisfies relations in } R} \rangle$, $\widehat{s_i}$ = coset of s_i.

(iii) $\implies |G'| \leq n \implies \overline{\varphi}$ bijective $\implies \ker\varphi = N$ □

Example 1.29.5

- $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$
  $\forall G = \langle x, y \rangle$ with $x^n = y^2 = 1$, $xy = yx^{-1} \implies G = \{x^i, yx^i\} \implies |G| \leq 2n$.
- $Q = \langle i, j \mid i^4 = 1, j^2 = i^2, ij = ji^{-1} \rangle$
- $C_n \times C_m \cong \langle x^n = y^m = 1, xy = yx \rangle$

Remark: $\mathbb{Z} \cong F(\{x\})$



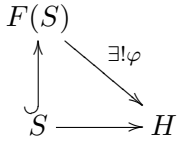
such that $\varphi(1) = f(x)$, define $\varphi(n) = f(x)^n$.
Exercise: $\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid xy = yx \rangle$.

Notation: If $r = x_1^{e_1} \cdots x_n^{e_n} \in R$, if H is any group $h_1 \cdots h_n \in H$, $r(h_1 \cdots h_n) = h_1^{e_1} \cdots h_n^{e_n}$.

Proposition 1.29.6
If $G = \langle s_1, \ldots, s_n \mid r_1, \ldots, r_n$, the to give $G \xrightarrow{f} H$ a homomorphism is equivalent to giving $h_1, \ldots, h_n \in H$ satisfying $r_i(h_1 \cdots h_n) = 1 \ \forall i = 1, \ldots, k$.

Proof
($\implies$) Clear: Let $h_i = f(s_i)$.
Then $r_i(s_1 \cdots s_n) = 1 \implies \underbrace{f(r_i(s_1 \cdots s_n))}_{r_i(h_1 \cdots h_n)} = f(1) = 1 \implies r_s(h_1 \cdots h_n) = 1$.

($\Leftarrow$) Let $h_1 \cdots h_n \in H$ such that $r_i(h_1 \cdots h_n) = 1$ for all i



N:= normal subgroup of $F(S)$ generated by $R = \{r_1, \ldots, r_n\}$ $\varphi(s_i) = h_i$

Know $G \cong F(S)/N$ ($G - \langle S, R \rangle$). Prove: $N \subseteq \ker(\varphi)$:

$$r_i(h_1 \cdots h_n) = 1 \iff r_i \in \ker\varphi$$

$\implies N \subseteq \ker\varphi \implies \varphi$ factors through $G \cong F(S)/N \to H$. □

Corollary 1.29.7
If $\langle h_1 \cdots h_n \rangle = H$, then $f : G \to H$ is surjective. (f as in prop)

Example 1.29.8
Give $D_{2n} \to H \iff$ give $x, y \in H$ such that $x^n = y^2 = 1$, $xy = yx^{-1}$.

Example 1.29.9
$Q_n = \langle a, b \mid a^{2^{n-1}} = 1, ba = a^{-1}b, b^2 = a^{2^{n-1}} \rangle$ generalised quaternion group. $(Q_3 = Q)$
$|Q_n| = 2^n$.
Easy, $Q_n\{a^i, a^ib \mid 0 \leq i \leq 2^{n-1} - 1\} \implies |Q_n \leq 2^n|$

$$\begin{matrix} a^{i_1}b & a^{i_2}b \\ a^i & a^ib \end{matrix}$$

Define $f : Q \to GL_2(\mathbb{C})$ by
$f(a) = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix}$ $\xi = \xi_{2^{n-1}}$ root of 1.
$f(b) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ $(\xi_m = e^{\frac{2\pi i}{m}}$ mth root of 1).

Prop. $\implies$ f is a group hom

$$h_n(f) = \left\{ \begin{bmatrix} \xi^i & 0 \\ 0 & \xi^{-i} \end{bmatrix} \begin{bmatrix} 0 & \xi^i \\ \xi^{-i} & 0 \end{bmatrix} \right\}$$

has 2^n elements. $0 \leq i \leq 2^{n-1} - 1 \implies |Q_n| = 2^n$.

2 Commutative Rings and Their Modules

Recall that a ring is a set R with operations $+, \cdot$ such that

(i) $(R, +)$ abelian

(ii) $(R, \cdot)$ is associative and distributive, $a(bc) = (ab)c$, $a(b + c) = ab + ac, (a + b)c = ac + bc$,

R is commutative if $ab = ba$, $a, b \in R$. R has an identity if $\exists 1 \in R$ such that $a \cdot 1 = 1$, $a = a$ $\forall a \in R$.

Now: R commutative with 1.
$\exists$ rings with out 1: $2\,\mathbb{Z}/$

Example 2.0.10
The zero ring 0, $\mathbb{Z}$, any field is a ring: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.

Recall that a ring R is a field if $1 \neq 0$ and R is commutative with $(R \setminus \{0\}, \cdot)$ is a group.
Remark: R a ring, $1 = 0 \iff R = 0$.

Example 2.0.11
R ring $\rightsquigarrow$ form polynomial rings: $R[X], R[X_1, \ldots, X_n]$

Example 2.0.12
$\{R_i\}_{i \in I}$ rings $\implies \prod_{i \in I} R_i = \{(r_i)_{i \in I} \mid r_i \in R_i\}$.

Definition 2.0.13
A map $f : R \to R'$ is a ring homomorphism if for all x, y

(i) $f(x + y) = f(x) + f(y)$

(ii) $f(xy) = f(x)f(y)$

(iii) $f(1_R) = 1_{R'}$

Example 2.0.14

- The only ring homomorphism $f : \mathbb{Z} \to R$ is

$$n \longmapsto n \cdot 1_R = \underbrace{1_R + \cdots + 1_r}_{n \text{ times}} \qquad (n > 0)$$

  $\forall f : \mathbb{Z} \to R$, $f(1) = 1_R$

- $\begin{matrix} f : R \to 0 \\ x \mapsto 0 \end{matrix}$ $\forall x \in R$ is a ring hom.
  But $g : 0 \to R$ by $0 \mapsto 0$ is not a ring hom, unless $R = 0$. ($1_0 = 0 \not\mapsto 1_R$)
- Evaluation map at $a_1, \ldots, a_n$.

$$\begin{aligned} f : R[X_1, \ldots, X_n] &\to R \\ x_i &\mapsto a_i \in R, \quad i = 1, \ldots, n \\ f(P(X_1, \ldots, X_n)) &= P(a_1, \ldots, a_n), \quad \forall P \in R[X_1, \ldots X_n] \end{aligned}$$

- $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$.

Definition 2.0.15
R a ring. An R-module is an abelian group $(M, +)$ together with $\cdot : R \times M \to M$ such that for all $r_1, r_2 \in R$, $m \in M$:

(i) $r_1(r_2 m) = (r_1 r_2)m$

(ii) $(r_1 + r_2)m = r_1 m + r_2 m$

(iii) $r(m_1 + m_2) = rm_1 + rm_2$

(iv) $1_R \cdot m = m$

Example 2.0.16

- $R = \mathbb{Z}$, $\mathbb{Z}$-modules = abelian groups. G an abelian group:

$$n \cdot x = \underbrace{x + \cdots + x}_{n \text{ times}} \qquad (n > 0)$$

  $n_1 \cdot (n_2 \cdot x) = (n_1 n_2) \cdot x$

- $R = F$ a field. F-modules = F-vector spaces.
- $F[X]-$modules $\iff$ F-vector spaces V together with linear map $T : V \to V$.
  ($\Rightarrow$) M an $F[X]-$module $\implies$ take $V = M$ is an F-vecotr space.

$$T : V \to V, \quad T(v) = x \cdot v \quad \forall v \in V$$

  is a T-linear map.
  T-linear: $X(v_1 + v_2) = X \cdot v_1 + X \cdot v_2$ is just

$$T(v_1 + v_2) = T(v_1) + T(v_2)$$

$$\underbrace{X \cdot (\lambda v)}_{T(\lambda v)} = \underbrace{\lambda (Xv)}_{T(v)}$$

Example 2.0.17
$R^n = \{(x_1, \ldots, x_n) \mid x_i \in R\}$ is an R-module.
$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$.

Definition 2.0.18
R ring, $S \subseteq R$ is a subring if $(S, +, \cdot)$ is a ring in its own right. (not necessarily with 1).
$I \subseteq R$ is an ideal if $(I, +) \leq (R, +)$ and $\forall x \in R$, $\forall y \in I$, $x \cdot y \in I$. ($\implies$ $(I, +, \cdot)$ subring.) We write $I \leq R$.
Remark: I ideal in $R \implies R/I$ is a ring.

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I) \cdot (y + I) = (xy) + I$$

Exercise: $(R/I, +, \cdot)$ is ring.

In fact, R/I is an R-module: $x \in R$, $x \cdot (y + I) = xy + I$
Well-defined: $x \cdot (y' + I) = xy' + I$

$$y + I = y' + I \iff y - y' \in I \implies xy - xy' \in I$$

Axioms:

$$x_1(x_2 \cdot (y + I)) = (x_1x_2)(y + I)$$
$$x_1(x_2y + I) = (x_1x_2)y + I$$
$$x_1(x_2y) + I = (x_1x_2)y + I$$

$$x(y_1 + y_2) = x((y_1 + I) + (y_2 + I)) = x(y_1 + I) + x(y_2 + I) = (xy_1 + xy_2) + I$$

R/I has a 1 if R has a 1: $(1 + I)$.

Definition 2.0.19
M, N R-modules.
An R-module homomorphism (R-linear) is a map $f : M \to N$ such that $\forall r \in R$, $m, m_1, m_2 \in M$

$$f(m_1 + m_2) = f(m_1) + f(m_2)$$
$$f(r \cdot m) = r \cdot f(m)$$

Example 2.0.20

- $0 : M \to N$, $x \mapsto 0$ $\forall x$.

$$0_R \cdot m = 0_M \quad \forall m \in M$$
$$r \cdot 0_M = 0_M \quad \forall r \in R$$

- $R = F$ a field. F-linear map = linear transformation between F-vector spaces
- What are the R-linear maps $R^n \xrightarrow{f} R^k$? $\vec{e_i} \mapsto \vec{a_i}$.

$$f(x_1, \ldots, x_n) = \sum x_i \vec{a_i}$$
$$= A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$A = [\vec{a_1}, \ldots, \vec{a_n}] \in M_{k\times n}(R)$.

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \sum x_i \vec{e_i}$$
$$\lambda\vec{e_i} = (0, \ldots, 0, \lambda, 0, \ldots, 0)$$

$\forall f : R^n \to R^m$ R-linear maps:

$$f(\vec{x}) \to f(\sum x_i\vec{e_i}) = \sum f(x_i\vec{e_i}) = \sum x_i f(\vec{e_i}) = \sum x_i\vec{a_i}$$

$\forall A \in M_{k\times n}(R)$, $f(\vec{x}) = A\vec{x}$ is R-linear.

$$A(\vec{x} + \vec{y}) = A\vec{x} + A\vec{y}$$
$$A(\lambda\vec{x} = \lambda(A\vec{x}))$$

2.1 Elements of Category Theory

Definition 2.1.1
A category $\mathcal{C}$ consists of:

I. a class of objects $\mathrm{Obj}(\mathcal{C})$

II. for all $A, B \in \mathrm{Obj}(\mathcal{C})$ a set, $\mathrm{Mor}_{\mathcal{C}}(A, B)$ of morphisms ("arrows", $A \to B$)

III. $\forall A, B, C \in \mathrm{Obj}(\mathcal{C})$, a function

$$\mathrm{Mor}_{\mathcal{C}}(A, B) \times \mathrm{Mor}_{\mathcal{C}}(B, C) \to \mathrm{Mor}(A, C) \qquad (\text{"composition"})$$
$$(A \xrightarrow{f} B, B \xrightarrow{g} C) \mapsto A \xrightarrow{g\circ f} C$$

such that

(i) $\mathrm{Mor}(A, B)$, $\mathrm{Mor}(A', B')$ disjoint unless $A = A'$, $B = B'$

(ii) $h \circ (g \circ f) = (h \circ g) \circ f$

(iii) $\forall A \in \mathrm{Obj}(\mathcal{C})$, $1_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$ such that $f \circ 1_A = f = 1_a \circ f \quad \forall f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$

Example 2.1.2

- $\mathcal{C}$ =**Set**, Objects = Sets, Mor = functions
- $\mathcal{C}$ =**Grp**, Objects = Groups, Mor = group homs
- $\mathcal{C}$ =**Ab**, Objects = Abelian groups, Mor = groups homs
- $\mathcal{C}$ =**Ring**, Objects = Rings, Mor = ring homs
- R a ring. $\mathcal{C} = R$-**Mod**, Objects = R-modules, Mor = R-linear maps
- F a field. $\mathcal{C} = F$-**Mod**, Objects = F-vector spaces, Mor = F-linear maps
- $\mathcal{C}$ = **Top**, Objects = Topological Spaces, Mor = continuous maps

Definition 2.1.3
$\mathcal{C}, \mathcal{D}$ categories. A covariant functor $F : \mathcal{C} \to \mathcal{D}$ consists of:

(i) a map $F : \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$

(ii) $\forall A, B \in \mathrm{Obj}(\mathcal{C})$ a function

$$F : \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{D}}(F(A), F(B))$$

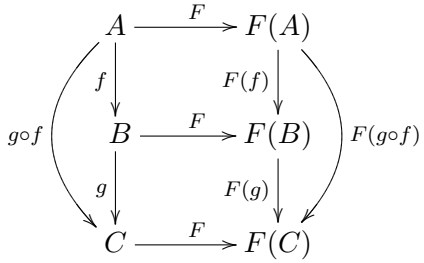
such that

$$f : A \to B \mapsto F(f) : F(A) \to F(B)$$

such that

(a) $F(1_A) = 1_{F(A)}$

(b) $F(g \circ f) = F(g) \circ F(f)$



Example 2.1.4

- Forgetful functors, for example:

$$\begin{aligned} F &: \mathbf{Grp} \to \mathbf{Set} \\ G \ \ \text{group} &\mapsto G \text{ underlying set} \\ f &: G \to H \\ \text{group hom} &\mapsto \text{underlying map} \end{aligned}$$

- $F =$ field, V an F-vector space.

$$\begin{aligned} \mathrm{Hom}_F(V, -) : F\text{-}\mathbf{Vect} &\to F\text{-}\mathbf{Vect} \\ W &\mapsto \mathrm{Hom}_F(V, W) \\ (W \xrightarrow{f} W') &\mapsto \big(\mathrm{Hom}_F(V, W) \to \mathrm{Hom}_F(V, W')\big) \\ (V \xrightarrow{g} W) \mapsto (V \xrightarrow{f \circ g} W') &\rightsquigarrow g \mapsto f \circ g \end{aligned}$$

More generally, $\mathcal{C} =$category, $A \in \mathrm{Obj}(\mathcal{C})$.
Define a covariant functor:

$$\begin{aligned} & M(A, -) : \mathcal{C} \to \mathbf{Set} \\ \mathrm{Obj}: \quad & B \mapsto \mathrm{Mor}(A, B) \\ \mathrm{Mor}: \quad & (B \xrightarrow{f} B') \mapsto (\mathrm{Mor}(A, B) \to \mathrm{Mor}(A, B')) \\ & (B \xrightarrow{f} B') \rightsquigarrow \Big((A \xrightarrow{g}) \mapsto (A \xrightarrow{f \circ g} B')\Big) \end{aligned}$$

Example 2.1.5
$\mathcal{C} = R\text{−}\mathbf{mod}$, $M = R$−module

$$\begin{aligned} \mathrm{Hom}_R(M, -) : R\text{-}\mathbf{mod} &\to R\text{-}\mathbf{mod} \\ N &\mapsto \mathrm{Hom}_R(M, N) \end{aligned}$$

Remark: M, N $R-$modules. $\mathrm{Hom}_R(M,N) = \{f : M \to N \mid R\text{-linear}\}$ is an $R-$module.

Particular Cases
- $M^* = \mathrm{Hom}_R(M,R)$ is the dual of M
- $\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$

Definition 2.1.6
A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is an "arrow-reversing" functor.

$$F : \mathrm{Mor}_{\mathcal{C}}(A,B) \to \mathrm{Mor}_{\mathcal{D}}(F(B),F(A))$$
$$A \xrightarrow{f} B \xrightarrow{g} C \rightsquigarrow F(C) \underbrace{\xrightarrow{F(g)} F(B) \xrightarrow{F(f)}}_{F(g\circ f)} F(A)$$

$\mathrm{Hom}_R(-,N)$ is contravariant.
Generally, $\mathcal{C}$ a category, $A \in \mathrm{Obj}(\mathcal{C})$:

$$Mor(-,A) : \mathcal{C} \to \mathbf{Set}$$
$$B \mapsto \mathrm{Mor}(B,A)$$
$$(B \xrightarrow{f} B') \rightsquigarrow \big(\mathrm{Mor}(B',A) \to \mathrm{Mor}(B,A)\big)$$
$$(B' \xrightarrow{g} A) \mapsto (B \xrightarrow{g\circ f} A)$$

2.2 An example of a covariant functor for modules

Change of Ring
$\varphi : R' \to R$ ring homomorphism. M an R-module. M is also an R'-module via:

$$r' \cdot m = \varphi(r')m$$

and we write ${}_{R'}M, \varphi^*M$.
Check axioms:

(i) $r'_1 \cdot (r'_2 \cdot m) = r'_1 \cdot (\varphi(r'_2)m) = (\varphi(r'_1)\varphi(r'_2))m = \varphi(r'_1 r'_2)m = (r'_1 r'_2)m$

(ii) $r'(m_1 + m_2) = \varphi(r_1)(m_1 + m_2) = \varphi(r')m_1 + \varphi(r')m_2 = r'_1 m_1 + r'_2 m_2$

(iii) exercise

(iv) $1_{R'} = \varphi(1_{R'})m = 1_R \cdot m = m$

If $f : M \to N$ is R-linear, then the same map on the underlyinig sets is R'-linear:

$$f' :_{R'} M \to_{R'} M \qquad (f' = f)$$

$f'(r' \cdot m) = \varphi(r')m = \varphi(r')f(m) = r' \cdot f'(m)$.
This gives a functor:

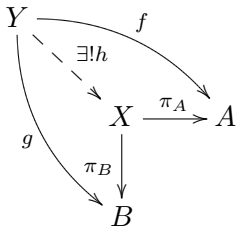
$$\varphi : R\text{-}\mathbf{mod} \longrightarrow R'\text{-}\mathbf{mod}$$
$$M \longmapsto_{R'} M$$
$$(f : M \to N) \longmapsto (f' :_{R'} M \to_{R'} N)$$

Definition 2.2.1
M an R-module. An $\underline{R\text{-submodule}}$ of M is the obvious thing: a subset $N \subseteq M$ such that $(N, +, \cdot)$ is a module, i.e. $(N, +) \leq (M, +)$, N closed under $\cdot$.

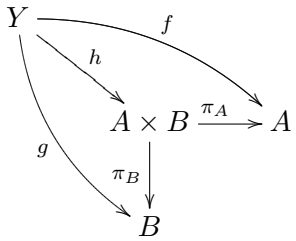
Example 2.2.2
R a ring. R as an R-module, then the submodules of R is precisely the ideals of R.

2.3 Products & Coproducts

Products
$\mathcal{C}$ a category. If $A, B \in \text{Obj}(\mathcal{C})$, then a $\underline{\text{a product of } A, B \text{ in } \mathcal{C}}$ (if it exists) is an object X and 2 maps $\pi_A : X \to A$, $\pi_B : X \to B$ satisfies the "universal property":
$\forall Y \in \text{Obj}(\mathcal{C})$ and maps $f : Y \to A$, $g : Y \to B$, $\exists! h : Y \to X$ such that $f = \pi_A \circ h$, $g = \pi_B \circ h$.



Example 2.3.1
$\mathcal{C}$=**Set**. $X = A \times B$ product of A and B. $\begin{matrix}\pi_A : X \to A \\ \pi_B : X \to B\end{matrix}$ with $\begin{matrix}\pi_A(a,b) = a \\ \pi_B(a,b) = b\end{matrix}$.
Given f, g, $h(y) = a_y b_b = f(y)b(y)$.



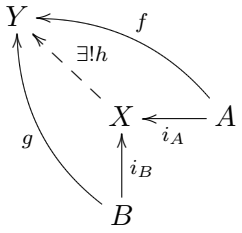
$\pi_A \circ h(y) = f(y),\ a_y = f(y).$

Exercise: $\nexists$ product in the category of fields.

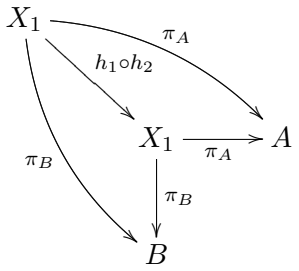
Similarly, we can define product, X, of objects $\{A_i\}_{i \in I}$ in $\mathcal{C}$. $\pi_i : X \to A_i$

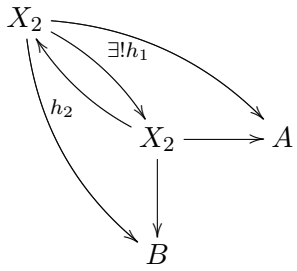
Coproducts

If $A, B \in \text{Obj}(\mathcal{C})$, then a $\underline{\text{coproduct}}$ of A, B in $\mathcal{C}$ (if it exists) is an object X with 2 maps $\begin{matrix}i_A : A \to X \\ i_B : B \to X\end{matrix}$
such that $\forall Y \in \text{Obj}(\mathcal{C})$ and maps $\begin{matrix}A \xrightarrow{f} Y \\ B \xrightarrow{g} Y\end{matrix}$, $\exists! h : X \to Y$ such that $\begin{matrix}f = h \circ i_A \\ g = h \circ i_B.\end{matrix}$



Example 2.3.2
$\mathcal{C}=$ Set. $A \sqcup B=$ coproduct of A and B.
Remark: If the product, coproduct exists, it is unique up to isomorphism.
i.e. $A \underset{g}{\overset{f}{\rightleftarrows}} B$ such that $\begin{matrix} f \circ g = 1_B \\ g \circ f = 1_A \end{matrix}$.





2.4 Modules: Sums and Products

$\{M_i\}_{i \in I}$ collection of R-modules.
Direct Sum

$$\bigoplus_{i \in I} M_i = \{(m_i) \mid m_i \in M_i, \text{ all but finitely many } 0\}$$

Direct Product

$$\prod_{i \in I} M_i = \{(m_i) \mid m_i \in M_i\}$$

Remark: If $|I| < \infty$. $\bigoplus M_i = \prod M_i$.

Proposition 2.4.1

(i) $\prod M_i$ is a product of $\{M_i\}_{i \in I}$ in R-mod.
(ii) $\bigoplus M_i$ is a coproduct in R-mod.

Proof

□

Sum:
R a ring. $N, N' \leq M$ then

$$N + N' = \{x + y \mid n \in N, n' \in N'\}$$

is a submodule of M.
(This is just the additive notation of $HK \leq G$.)

$$\begin{matrix} N \times N' \xrightarrow{f} N + N' \leq M \\ (x, y) \mapsto x + y \end{matrix}$$

Multiplicatively:

$$\begin{matrix} H \times K \to HK \subseteq G(\text{abelian}) \\ (x, y) \mapsto xy \end{matrix}$$

f is R-linear: $f(r(x,y)) = f(rx, ry) = rx + ry = r(x+y) = r(f(x,y))$.

Definition 2.4.2
$f : M \to N$ R-linear. $\ker(f) = \{m \mid f(m) = 0\}$.

$\ker(f) = \{(x,y) \mid x + y = 0\} = \{(x,-x) \mid x \in N \cap N'\}$. If $N \cap N' = \{0\}$, then f is an isomorphism of R-modules.
(Exercise: Bijective R-linear maps $\iff$ isomorphism in $\underline{R\text{-}\mathbf{mod}}$)
Then $N \times N' \cong N + N'$. $N + N'$ is called an internal direct product of N and N' if the map $f : N \times N' \to N + N'$ is an isomorphism ($\iff$ $N \cap N' = \{0\}$).
Remark: This is the product/direct sum.

Definition 2.4.3
M and R-module, $\{M_i\}_{i \in I}$ submodules. M if an internal direct sum of $\{M_i\}$ if

$$\begin{aligned} \bigoplus M_i &\to M \\ (m_i) &\mapsto \sum m_i \end{aligned}$$

is an isomorphism.

2.5 Quotient Modules

R a ring, $N \leq M$ an R-module, then the abelian group

$$M/N = \{m + N \mid m \in M\}$$

is an R-module via:

$$r \cdot (m + N) = rm + N$$

Well-defined:

$$\begin{aligned} & m + N = m' + N \\ \implies \quad & m - m' \in N \\ \implies \quad & rm - rm' \in N \\ \implies \quad & rm + N = rm' + N \end{aligned}$$

Axioms:

(i) $r_1(r_2(m+N)) = r_1(r_2 m + N) = r_1(r_2 m) + N = (r_1 r_2)(m+N)$
(iv) $1 \cdot (m+N) = 1 \cdot m + N = m + N$.

$\pi : M \to M/N$ by $\pi(m) = m + N$ is R-linear.

M an $R-$module. Write $N \leq_R M$ (or $N \leq M$) for N $R-$submodule. e.g. $I \leq R$ ideal in R.

Recall that for $N, N' \leq M$, $N + N' = \{x + y \mid x \in N, y \in N'\} \leq M$. More generally, if $\{N_i\}_{i \in I}$ are submodules of M,

$$\sum N_i := \{\sum n_i \mid n_i \in N_i, \text{ all but finitely many } 0\} \leq M$$

Direct sum:

$$\bigoplus_{i \in I} N_i = \{(n_i) \mid n_i \in N_i, \text{ all but finitely many } 0\} \subseteq \prod_{i \in I} N_i$$

$\exists f : \prod_{i \in I} N_i \to \sum N_i$, $f((x_i)) = \sum n_i$.

Exercise: f is $R-$linear and surjective.

$\sum N_i$ is an internal direct sum if f is an isomorphism
$\iff \forall n \in \sum N_i, \exists! n_i \in N_i$ such that $n = \sum n_i$
$\iff \forall i,\ N_i \cap \sum_{j \neq i} N_j = \{0\}$.

M an $R-$module is generated by $\{m_i\}_{i \in I}$ if $M = \sum_{i \in I} Rm_i$ for some $m_i \in M$, where $Rm = \{rm \mid r \in R\} \leq M$. We write $M = \langle m_i \mid i \in I \rangle$

M is finitely generated if $M = \langle m_1, \dots m_k \rangle$ for some $m_i \in M$. For example, $Rm = \langle m \rangle$.

Definition 2.5.1
M is cyclic if $M = \langle m \rangle$ for some $m \in M$.
Remark:

- $\mathbb{R} = \mathbb{Z}$, f.g. $\mathbb{Z}-$modules = f.g. abelian groups, cyclic $\mathbb{Z}-$modules = cyclic abelian groups
- $R = k$ field, f.g. $k-$modules = finite dimensional $k-$vector spaces

M f.g. $R-$module $\iff \exists R^k \twoheadrightarrow M$ surjective and $R-$linear.

Proof
$(\Rightarrow)$ $M = \langle m_1, \dots, m_k$. Let $f : R^k \to M$, $e_i \mapsto m_i$. $f(r_1, \dots, r_k) = \sum r_i m_i$.
Exercise: f is $R-$linear and surjective.

$(\Leftarrow)$ Let $m_i = f(0, \dots, 0, \underbrace{1}_{i\text{th}}, 0, \dots, 0)$. Then $f(r_1, \dots, r_k) = \sum r_i m_i$ since f is $R-$linear. f surjective $\implies M = \langle m_1, \dots, m_k \rangle$. □

Remark:

- M f.g. $R-$module $\iff M \equiv R^k/N$ for some $N \leq R^k$
- M is cyclic $\iff \exists R \twoheadrightarrow M$ $R-$linear, surjective $\iff M \cong R/I$ for some ideal $I \leq R$.

2.6 Isomorphism Theorems For Modules

Theorem 2.6.1 (First Isomorphism Theorem)
$f : M \to N$, $R-$linear $\implies \ker f \leq M$, $\mathrm{Im}(f) \leq N$. f induces an isomorphism of $R-$modules

$$\overline{f} : M/\ker f \to \mathrm{Im}\, f$$
$$\overline{f}(x + \ker f) = f(x)$$

Remark:

- $f : M \to N$ $R-$linear, $N' \leq N \implies f^{-1}(N') \leq M$. (Closed under $\cdot$: $x \in f^{-1}(N)$, $x \in R \implies r \cdot x \in f^{-1}(N')$, $f(r \cdot x) = rf(x)$)
- $\pi : M \twoheadrightarrow N$ surjective $R-$linear $\exists$ 1-1 correspondence

$$\{\text{Submodules of } N\} \leftrightarrow \{\text{Submodules of } M \text{ that contain } \ker \pi\}$$

- First Iso $\implies N \cong M/\ker \pi$. More generally, if $M' \leq M$ and let $\pi : M \to M/M'$ quotient map.

$\exists$ 1-1 correspondence

$$\{\text{Submodules of } M/M'\} \leftrightarrow \{\text{Submodules } \widetilde{M} \leq M,\ M' \leq \widetilde{M}\}$$
$$K \leq M/M' \mapsto \pi^{-1}(K)$$
$$\pi(\widetilde{M}) = \widetilde{M}/M' \hookleftarrow \widetilde{M}$$

- $N_i \leq M,\ i \in I \implies \bigcap_{i\in I} N_i \leq M$

Theorem 2.6.2 (Second Isomorphism Theorem)
$N_1, N_2 \leq M$. Then

$$N_1/(N_1 \cap N_2) \cong (N_1 + N_2)/N_2$$

isomorphism of $R-$modules.
(Recall $H, K \leq G$ then $H/(H \cap K) \cong HK/K$)

Proof

$$N_1 \overset{f}{\hookrightarrow} N_1 + N_2 \longrightarrow N_1 + N_2/N_1$$

$f(x) = x + N_2$ $R-$linear.

$$\ker f = \{x \in N_1 \mid x \in N_2\} = N_1 \cap N_2$$

First isom $\implies$ $N_1/N_1 \cap N_2 \cong N_1 + N_2/N_2$. □

Theorem 2.6.3 (Third Isomorphism Theorem)
If $M_3 \leq M_2 \leq M_1$ then

$$(M_1/M_3)/(M_2/M_3) \cong M_1/M_2$$

isomorphism of $R-$modules.

Proof
f is $R-$linear: $f(r \cdot (x + M_3)) = f(rx + M_3) = rx + M_2 = r(x + M_2)$
$\ker f = \{x + M_3 \mid x \in M_2\} = M_2/M_3$.
First isom $\implies$

$$(M_1/M_3)/(M_2/M_3) \cong M_1/M_2.$$

□

2.7 Isomorphism Theorems For Rings

Theorem 2.7.1 (First Isomorphism Theorem)
$f : R \to S$ ring homomorphism $\implies$ $\ker f \leq R$, $\mathrm{Im}(f)$ is a subring of S. The map

$$\overline{f} : R/\ker f \to \mathrm{Im}(f)$$
$$\overline{f}(x + \ker f) = f(x)$$

is an isomorphism of rings.

Proof
S is an $R-$module via $r\cdot = f(r)s$. Then f is $R-$linear $\implies \ker f \leq R$.
$\operatorname{Im} f$ is a subring: $f(x), f(y) \in \operatorname{Im}(f) \implies f(x)f(y) = f(xy) \in \operatorname{Im} f$
$\overline{f}$ is a hom of rings: $\overline{f}((x+\ker f)(y+\ker f)) = \overline{f}(xy+\ker f) = f(xy) = f(x)f(y) = \overline{f}(x+\ker f)\overline{y+\ker f}$ □

Theorem 2.7.2 (Second Isomorphism Theorem)
$I \leq R$, $S \subseteq R$ subring $\implies$

$$I + S = \{x + y \mid x \in I, y \in S\}$$

is a subring of R, and $(I+S)/I \cong S/I \cap S$ ismorphism of ring.

Proof
$I + S$ closed under $\cdot$: $x_1, x_2 \in I$, $y_1, y_2 \in S$,

$$(x_1+y_1)(x_2+y_2) = \underbrace{x_1(x_2+y_2)}_{\in I} + \underbrace{x_2y_1}_{\in I} + \underbrace{y_1y_2}_{\in S} \in I+S$$

$I \subseteq I+S \subseteq R$, $I \cap S \subseteq S$.

$$S \underset{\text{ring hom.}}{\hookrightarrow} I+S \underset{\text{ring hom.}}{\longrightarrow} (I+S)/I \qquad (S \xrightarrow{\quad f \quad} (I+S)/I)$$

$f(x) = x + I$ ring hom, surjective.

$$\ker f = I \cap S \implies S/I \cap S \cong I + S/I$$

by first isom. In particular, if $I, J \leq R$, then $I + J \leq R$ and $I + J/I \cong J/I \cap J$ isom of rings. □

Theorem 2.7.3 (Third Isomorphism Theorem)
$I \leq J \leq R$. $(R/I)/(J/I) \cong R/J$ isomorphism of rings.

Proof
$R/I \xrightarrow{f} R/J$, $f(x+I) = (x+J)$. Exercise: f surjective of rings, $\ker f = J/I$. □

2.8 Subrings of Fields as a Source of Rings

Example 2.8.1

- $\mathbb{Z} \subseteq \mathbb{Q}$
- $\mathbb{Z}[\frac{1}{p+1}, \ldots, \frac{1}{p_k}] = \{\frac{x}{s} \mid s = \pm p_1^{l_1} \cdots p_k^{l_k}, l_i \geq 0 \text{ integers}\} \subseteq \mathbb{Q}$ e.g. $\mathbb{Z}[\frac{1}{2}], \mathbb{Z}[\frac{1}{3}]$
- $\mathbb{Z}_{\langle p \rangle} = \{\frac{x}{s} \mid p \nmid s\} \subseteq \mathbb{Q}$ for prime p.

Definition 2.8.2
R is an integral domain if it is a commutative ring with $xy = 0 \implies x = 0$ or $y = 0$ for any $x, y \in R$.

Field of Fractions $\operatorname{Frac}(R)$
R an integral domain. Construct a field $F(R)$ with $R \hookrightarrow F(R)$. (analogous fo $\mathbb{Z} \subseteq \mathbb{Q}$).

$$\operatorname{Frac}(R) := \{(r, s) \mid r \in R, s \in R \setminus \{0\}\}/\sim$$

where $(r_1, s_1) \sim (r_2, s_2) \iff s_2 r_1 = s_1 r_2$. Let $\frac{r}{s} :=$ equivalence class of (r, s).
$\sim$ is an equivalence relation:
$(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$
$(r_2, s_2) \sim (r_3, s_3) \iff r_2 s_3 = r_3 s_2$ $\implies r_3 s_1 = r_1 s_3$.
$r_1(r_2 s_3) = r_3 r_1 s_2 = r_2(r_3 s_1)$. For $r_2 \neq 0$, R integral domain so $(r_1, s_1) \sim (r_3, s_3)$. (Exercise: Let $r_2 = 0$).

2.9 Ring of Fractions

Remark: K a field, R ring $\subseteq K$, then R is integral domain.

Given R an inegral domain, construct a field $\mathrm{Frac}(R)$ with $R \in \mathrm{Frac}(R)$ by analogy of construction of $\mathbb{Q}$ by $\mathbb{Z}$.

$$\mathrm{Frac}(R) = \{(t, s) \mid t \in R, s \in R \setminus \{0\}\} / \sim$$

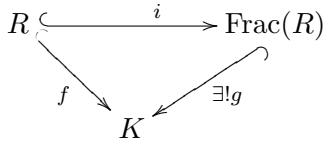
where $(t_1, s_1) \sim (t_2, m_2) \iff t_1 s_1 = t_2 s_1$, class written as $\frac{t}{s}$.

Addition and mulitplication are defined as follows:

$$\frac{t_1}{s_1} + \frac{t_2}{s_2} = \frac{t_1 s_2 + t_2 s_1}{s_1 s_2}$$
$$\frac{t_1}{s_1} \cdot \frac{t_2}{s_2} = \frac{t_1 t_2}{s_1 s_2}$$

Exercise: These operations are well-defined.

Proposition 2.9.1
$\mathrm{Frac}(R)$ has the universal property: $\forall f : R \hookrightarrow K$ injective hom, $K =$ field, $\exists! g : \mathrm{Frac}(R) \hookrightarrow K$ injective such that $f = g \circ i$



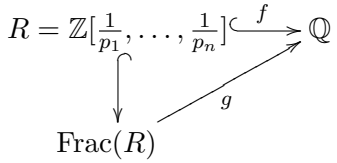
Proof
Let $g\left(\frac{t}{s}\right) = f(t) f(s)^{-1}$, $s \neq 0, f(s) \neq 0$.
g is unique such that $g \circ i = f$. $g\left(\frac{t}{1}\right) = f(t)$.

$$g\left(\frac{t}{s}\right) \cdot f(s) = g\left(\frac{t}{s}\right) \cdot g\left(\frac{s}{1}\right) = g\left(\frac{t}{1}\right) = f(t)$$

Exercise: g is well-defined and g is a ring hom.
Exercise$K$, L fields, any $f : K \to L$ nonzero is injective. □

Example 2.9.2

- $\mathrm{Frac}(\mathbb{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_n}]) = \mathbb{Q}$, so g is an isomorphism.



Proposition $\implies$ g is injective but g is surjective, $g(\frac{a/p_1}{b/p_1}) = \frac{a}{b}$.

- $R = k[x_1, \ldots, x_n]$ for a field k.
  $\text{Frac}(R) = k(x_1, \ldots, x_n) = \{\frac{P(x_1,\ldots,x_n)}{Q(x_1,\ldots,x_n)} \mid Q \neq 0\}$. - function field of dimension n

2.10 Prime and Maximal Ideals

Definition 2.10.1
An ideal $I \leq R$, $I \neq R$ is prime if $xy \in I \implies x \in I$ or $y \in Y$, maximal if $I \subseteq J \subseteq R \implies I = J$ or $J = R$.

Example 2.10.2

- $R = \mathbb{Z}$, $n\mathbb{Z} = (n)$ is prime $\iff$ n is prime or $n = 0$, maximal $\iff$ n is prime.
- (0) is prime in $R \iff R$ is an integral domain
- $k =$ field, $R = k[x]$, $f(x) \in k[x]$ irreducible $\implies$ $(f(x))$ is prime and maximal (proof later)
  $I \leq k[x]$ is prime $\iff$ $I = (f(x))$, $f =$ irreducible or $I = (0)$, maximal $\iff$ $I = (f(x))$, f irreducible.

Theorem 2.10.3
$I \leq R$, $I \neq R$, then

(i) I is prime $\iff$ R/I is an integral domain

(ii) I is maximal $\iff$ R/I is a field

In particular, maximal ideals are prime.

Proof

(i) I prime $\iff$ $xy \in I \implies x \in I$ or $y \in I$
$\iff$ $xy = 0$ in $R/I \implies x = 0$ in R/I or $y = 0$ in R/I
$\iff$ R/I integral domain

(ii) I maximal $\iff$ the only ideals of R/I are 0 and R/I

Claim: A ring R has no non-trivial ideals $\iff$ R is a field. □

Corollary 2.10.4
$f : K \to L$ hom of fields, ker $= 0$ (injective) or K (zero map).

Proof
Let $x \in R$, $x \neq 0$.
$(x) = \{rx \mid r \in R\} \neq 0$ principal ideal.
$(x) = R \iff 1 \in \langle x \rangle \iff \exists y \in R$ such that $yx = 1 \iff x$ has an inverse. □

Definition 2.10.5
A poset (partially ordered set) is a set P with a relation $<$ such that if $a < b$, $b < c$, then $a < c$. (possibly not every pair a, b is comparable.) We write $a \leq b$ for $a < b$ or $a = b$.

$P =$ poset, a subset $C \subset P$ is a chain if $x \leq y$ or $y \leq x$ $\forall x, y \in C$.

C is an upper bound if $\exists z \in P$ such that $\forall x \in C, x \leq z$.
P has a maximal z if $\nexists y \in P$ such that $z < y$.

Lemma 2.10.6 (Zorn's Lemma)
If P nonempty poset and every chain has an upper bound, then P has a maximal element.
Remark: Zorn's Lemma $\iff$ Axiom of Choice.

Theorem 2.10.7
R a ring with 1 then every proper ideal I of R is contained in a maximal ideal.

Proof
Let $X = \{J \leq R \mid J \neq R, J \supseteq I\}$. X poset with respect to inclusion.
If C is a chain in X, let $I' = \bigcup_{J \in C} J$. I' is an upper bound for C. $I' \in X$, $I' \leq R$: let $x, y \in I' \implies x \in I_1, y \in I_2$ for some $I_1, I_2 \in C$.
C chain $\implies I_1 \subseteq I_2$ or $I_2 \subseteq I_1$.
Say $I_1 \subseteq I_2$: $x \pm y \in I_2$.
$I' \neq R$: $1 \in I' \implies 1 \in J$ for some $J \in C$. Contradiction.
$\implies X$ has a maximal element. $\square$

2.11 Integral Domains

Definition 2.11.1

- $x \mid y$ if $y = rx$ for some $r \in R$ ($\iff y \in (x)$)
- $u \in R$ if a unit if $\exists v \in R$ such that $uv = 1$ ($u^{-1} = v$)
- $\pi \in R$ is irreducible if $\pi \neq 0$ or unit and $\pi = xy \implies x$ is a unit or y is a unit
- $\pi \in R$ is prime if $\pi \mid xy \implies \pi \mid x$ or $\pi \mid y$
- x and y are associates if $x \mid y$ and $y \mid x \iff (x) = (y) \iff x = uy$ for some unit u

Example 2.11.2

- π prime $\implies \pi$ irreducible:
  $\pi = xy \implies \pi \mid xy \implies \pi \mid x$ or $\pi \mid y$. Say $\pi \mid x$.
  Then $x = \pi x'$, $x' \in R \implies \pi = \pi x' y \implies x' y = 1 \implies y$ a unit
- In $\mathbb{Z}$, the units are ± 1, primes = irreducibles = $\{\pm 2, \pm 3, \pm 5, \ldots\}$. n is associated to $-n$.
- k = field, $R = k[x]$, primes = irreducibles = $\{f(x) \mid f$ irreducible$\}$
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
  $N(a + b\sqrt{-5}) = a^2 + 5b^2 = z \cdot \overline{z}$
  $N(\alpha\beta) = N(\alpha)N(\beta)$. Units = $\{\pm 1\}$

  2,3 are irreducible, but not prime
  $2 = \alpha\beta$ say, then:

$$4 = N(2) = N(\alpha)N(\beta) \implies N(\alpha), N(\beta) = 1, 2, 4$$
$$N(\alpha) \neq 2 \quad \forall \alpha$$

$\implies N(\alpha) = 1$ or $N(\beta) = 1 \implies \alpha$ is a unit or β is a unit.

$$2 \big| (1+\sqrt{-5})(1-\sqrt{-5}) = 6$$

but $2 \nmid 1 \pm \sqrt{-5}$, if $(1 \pm \sqrt{-5}) = 2(a + b\sqrt{-5})$
$\implies 4 = N(2) \big| N(1 \pm \sqrt{-5}) = 6$. Contradiction.

- $(R, \mathfrak{m})$ <u>local ring</u> if R has unique maximal ideal $\mathfrak{m}$. $\forall u \in R \setminus \mathfrak{m}$ is a unit.
  If $(u) \neq R$ then by theorem, $(u) \subseteq \mathfrak{m}$. Contradiction.
  If $(u) = R$, then u is a unit.
-

$$\begin{aligned} \pi \text{ prime} &\iff (\pi) \text{ is a prime} \\ &\iff \pi \big| xy \implies \pi \big| x \text{ or } \pi \big| y \\ &\iff xy \in (\pi) \implies x \in (\pi) \text{ or } y \in (\pi) \\ &\iff (\pi) \text{ is a prime ideal} \end{aligned}$$

2.12 Principal Ideal Domains

Definition 2.12.1
A domain R is a <u>PID</u> if every ideal is of the form (x) for some $x \in R$.
<u>Remark</u>: $(x) = (y) \iff x, y$ associates.

E.g. $\mathbb{Z}, k[x], \mathbb{Z}[i]$.
Non-e.g. $(2, x) \subset \mathbb{Z}[x]$, $(x, y) \subset k[x, y]$, $(2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$.

Definition 2.12.2
If $a, b \in R$ (ID), d is a <u>GCD</u> of (a, b) if $d \big| a$, $d \big| b$, and if $d' \big| a$ and $d' \big| b$, then $d' \big| d$.

If d and d' are both GCDs of a and b, $d' \big| d$ and $d \big| d' \implies d, d'$ are associates.
$(d = vd'$, $d' = ud \implies \not{d} = uv\not{d} \implies uv = 1)$
So $(d') = (d)$ and any d'' with $(d'') = (d)$ is a GCD of a, b.
So the <u>ideal</u> is unique: think of (d) as <u>the</u> GCD of a, b.

Proposition 2.12.3

- GCDs exist in PID
- If d is a GCD of a, b, then $\exists x, y \in R$ such that $ax + by = d$.

Proof
Consider $I = (a, b)$. Since R is a PID, I is principal, say $I = (d)$.
Claim: d is a GCD of a, b
$a \in (d) \implies d \big| a$, $b \in (d) \implies d \big| b$. $d \in (a, b) = \{ax + by \mid x, y \in R\}$, $d = ax + by$.
So if $d' \big| a, b \implies d' \big| ax + by = d$. So d is a GCD.
Any other GCD d' is $d' = du$, u a unit.
$\implies d' = du = (ax + by)u = axu + byu$. So it holds for d' as well. □

Proposition 2.12.4
In a PID, π irreducible $\iff \pi$ prime.

Proof
($\Rightarrow$) Suppose π is irreducible and $\pi \mid ab$. Suppose $\pi \nmid b$, we want to show $\pi \mid a$. Consider GCD(π, b). Divisors of π are units or (unit)$\cdot\pi$ - does not divide b.
So 1 is a GCD of π, b. Then $1 = \pi x + by \in R$.
$\implies a = \underbrace{\pi a x}_{\text{divisible by } \pi} + \underbrace{ab}_{\text{divisible by } \pi} y \implies \pi \mid a.$
($\Leftarrow$) Trivial, holds in any ring. □

2.13 Euclidean Domains

Definition 2.13.1
Euclidean domains are a special class of PIDs. Domain R is Euclidean if $\exists N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that $\forall f, g \in r$, $g \neq 0$, $\exists q, r \in R$ such that

- $f = qg + r$
- $r = 0$ or $N(r) < N(g)$

Example 2.13.2

- $R = \mathbb{Z}$ with $N(x) = |x|$
- $k[x], N(f) = \deg(f)$
- $\mathbb{Z}[i]$, $N(x + iy) = x^2 + y^2$

Theorem 2.13.3
Every Euclidean domain is a PID.

Proof
Suppose R Euclidean, $R \supset I$ ideal, $I \neq (0)$.

$$\emptyset \neq \{N(x) \mid x \in I \setminus \{0\}\} \subseteq \mathbb{Z}_{\geq 0}$$

So $\exists d \in I$ such that $N(d) \leq N(x)$, $\forall x \in I \setminus \{0\}$.
If $x \in I$ then $\exists q, r \in R$ such that

- $x = qd + r$
- $r = 0$ or ~~$N(x) \leq N(d)$~~

$d \in I, x \in I \implies r = x - qd \in I$. So if $r \neq 0$, $N(r) \geq N(d)$

$$\begin{aligned} &\implies r = 0 \\ &\implies d \mid x \\ &\implies I \subset (d), I \supset (d) \\ &\implies I = (d) \\ &\implies R \text{ is a PID} \end{aligned}$$

□

Corollary 2.13.4

(i) $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i]$ are PIDs

(ii) $\mathbb{Z}[x]$, $k[x]$, $\mathbb{Z}[i]$ are not Euclidean by considering the ideals $(2, x)$, (x, y), $(2, 1 + \sqrt{-5})$

Corollary 2.13.5
In $\mathbb{Z}$, prime ideals are (0), (p) - primes integers p.
In $k[x]$, prime ideals are (0), $(f(x))$, f irreducible non-constant.

Example 2.13.6
In $k[x, y]$, $(x - a, y - b)$ is prime $\forall a, b \in k$.

Proof
$(x - a, y - b)$ is kernel of $k[x, y] \to k$ by $x \mapsto a$, $y \mapsto b$, $f(x, y) \mapsto f(a, b)$. □

Example 2.13.7
In $\mathbb{Z}[i]$, the irreducibles are $a + ib \big| a^2 + b^2 = p_1 \cdots p_r$, so $a + bi \big| p$ for some $p \in \mathbb{Z}$.

(i) $\pm 1 \pm i$

(ii) $p \equiv 3 \bmod 4 \implies \pm p, \pm pi$

(iii) $p \equiv 1 \bmod 4 \implies p = a^2 + b^2 = (a + bi)(a - bi)$

$N(xy) = N(x)N(y)$.
$N(p) = p^2$, $xy = p \implies N(x)N(y) = p^2$, x, y non-units $\implies N(x) = N(y) = p$.

Example 2.13.8
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a non-Euclidean PID.
See Dummit and Foote P282 for proof.

Definition 2.13.9
$u \in R$ (non-unit) is a <u>universal side divisor</u> if $\forall x \in R$, either $u \big| x$ <u>or</u> $u \big| x +$ (unit).

Lemma 2.13.10
R Euclidean $\implies$ R has a universal side divisor.

Proof
N norm on R. Take $u \in R \setminus \{0\}, R^\times$ with smallest norm.
If $x \in R$ write $x = qu + r \implies$ either $r = 0 \implies u \big| x$ or $N(r) < N(u) \implies r$ a unit $\implies u \big| x - r$. □

<u>Sketch</u> Set $N\left(a + b(\frac{1+\sqrt{-19}}{2})\right) = a^2 + ab + 5b^2 = \left(a + b(\frac{1+\sqrt{-19}}{2})\right)\left(a + b(\frac{1-\sqrt{-19}}{2})\right)$
$\alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta}$.
$N(\alpha\beta) = N(\alpha)N(\beta)$.
Units are ± 1, so u is a USD $\implies u \big| x, x \pm 1 \ \forall x \in R$.

$x = 2 \implies u \big| 1, 2, 3 \implies u = \pm 2$ or ± 3.
$ab = 3 \implies N(ab) = N(a)N(b) = 9 \implies$ <u>$N(a), N(b) = 3$</u>

$x = \frac{1+\sqrt{-19}}{2}, x, x \pm 1$ not divisible by 2 or 3. $N(x) = 5$, $N(x \pm 1) = 7$.

Definition 2.13.11
R is <u>Noetherian</u> if R has the ascending chain condition on ideals. I.e. for all ideal chains $I_1 \subset I_2 \subset I_3 \subset \ldots$

in R, the chain stabilises: $\exists N \in \mathbb{Z}_{\geq 0}$ such that $I_n = I_N \ \forall n \geq N$.

This is a finiteness condition of R. e.g. fields, $\mathbb{Z}$ $(m) \subset (n) \iff n \big| m$.
R Noetherian $\implies$ R/I Noetherian for any I.

Proposition 2.13.12
R Noetherian $\iff$ every ideal is f.g.

Proof
($\Leftarrow$)Suppose $I_1 \subset I_2 \subset \ldots$ ascending chain. Let $I = \bigcup_n I_n$, so I is an ideal. $I = (x_1, \ldots, x_d)$, $\exists m$ such that $x_1, \ldots, x_d \in I_m \implies I \subset I_m$ but obviously $I_m \subset I$ so $I = I_m$ (chain stabilises after m).
($\Rightarrow$) Suppose I not f.g. Choose $x_1 \in I$, then $(x_1) \neq I$, choose $x_2 \in I \setminus (x_1)$, then $(x_1, x_2) \neq I \cdots$

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$$

$\implies$ R not noetherian. □

Corollary 2.13.13
All PIDs are noetherian.

Recall that every proper ideal in a ring R is contained in a maximal ideal. The proof required Zorn's Lemma. With Noetherian rings, we don't need to use Zorn's Lemma.

2.14 Structure of Prime Ideals in R

Definition 2.14.1
$\mathrm{Spec}(R) = \{\mathfrak{p} \mid \mathfrak{p} \text{ prime ideal in } R\}$.

E.g. $\mathrm{Spec}(\mathbb{Z}) = \{(p) \mid p \text{ prime}\} \cup \{0\}$, $\mathrm{Spec}(k[x]) = \{(f(x)) \mid f \text{ irreducible}\} \cup \{0\}$
More generally, if R is a PID, then

$$\mathrm{Spec}(R) = \{(\pi) \mid \pi \text{ prime}\} \cup \{0\} \qquad (\iff \text{irreducible})$$

Proof
If $\mathfrak{p} \neq 0$ prime in R a PID, $\mathfrak{p} = (\pi)$, $\pi \in R$. (π) prime $\iff$ π prime. □

$R = \mathbb{C}[X, Y]$, 3 kinds of prime ideals, (0), $(f(x, y))$ with f irreducible, $(x - a, y - b)$, $a, b \in \mathbb{C}$. Let $e_{a,b} : \mathbb{C}[X, Y] \to \mathbb{C}$, $f(x, y) \mapsto f(a, b)$, then $\ker e_{a,b} = (x - a, x - b)$ and $\mathbb{C}[X, Y]/(x - a, x - b) \cong \mathbb{C}$.
Remark: $(f(x, y)) \subseteq (x - a, x - b) \iff f(a, b) = 0$.

Definition 2.14.2
If $I \subseteq R$ is a set, we write $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}$. These form the closed sets of a topology on $\mathrm{Spec}(R)$, which is call the Zariski topology.
Remark: $I \subseteq J \implies V(J) \subseteq V(I)$.

(i) $V(R) = \emptyset$, $V((0)) = \mathrm{Spec}(R)$

(ii) $\bigcap_{j \in J} V(I_j) = V(\sum_{j \in J} I_j)$ because $\mathfrak{p} \in \bigcap V(I_j) \iff \mathfrak{p} \supseteq I_j \ \ \forall j \iff \mathfrak{p} \supseteq \sum I_j \iff \mathfrak{p} \in V(\sum I_j)$. ($\sum I_j$ is the smalest ideal containing all I_j)

(iii) $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$.
Suppose $\mathfrak{p} \in \bigcup_{j=1}^n V(I_j)$, then $\mathfrak{p} \supset V(I_j)$ for some j so $\mathfrak{p} \supset \bigcap_{i=1}^n I_j \implies \bigcup_{j=1}^n V(I_j) \subseteq V(\bigcap_{i=1}^n I_j)$.
Suppose $\mathfrak{p} \supset \bigcap_{j=1}^n I_j \supseteq \prod I_j \implies \mathfrak{p} \supset I_j$ for some j by primality of $\mathfrak{p}$.

So we have a topology.

Definition 2.14.3
$\mathrm{Rad}(I) = \sqrt{I} := \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$ is called the radical of I.
It can be shown that $\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 0}\}$. Remark: $I \subseteq \sqrt{I}$.
Remark: $V(\sqrt{I}) = V(I)$.

Proof
$I \subseteq \sqrt{I} \implies V(\sqrt{I}) \subseteq V(I)$.
Let $\mathfrak{p} \in V(I)$, $\mathfrak{p} \supseteq I$, then $\mathfrak{p} \supseteq \sqrt{I} = \bigcap_{\mathfrak{q} \supseteq I} \mathfrak{q}$. □

Definition 2.14.4
I is a radical ideal if $I = \sqrt{I}$.
e.g. $\mathfrak{p}$ prime $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

Claim: $\exists$ 1-1 correspondence

$$\{\text{radical ideals in } R\} \xleftrightarrow{1-1} \{\text{closed sets in } \mathrm{Spec}(R)\}$$
$$I \longmapsto V(I)$$

$$V(I) \subseteq V(J) \iff \sqrt{J} \subseteq \sqrt{I}$$
$$V(I) = V(J) \iff \sqrt{I} = \sqrt{J}$$

Theorem 2.14.5
$\exists$ 1-1 correspondence

$$\{\text{primes ideals in } R\} \xleftrightarrow{1-1} \{\text{irreducible closed sets in } \mathrm{Spec}\, R\}$$

Definition 2.14.6
A topological space is Noetherian if all chains of closed sets $C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$ stabilises.
Exercise: $\mathbb{R}$ with its usual topology is not Noetherian.

Lemma 2.14.7
R Noetherian ring $\iff$ $\mathrm{Spec}(R)$ Noetherian topological space.

Proof
Let $\mathbb{C}_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$ closed sets in $\mathrm{Spec}(R)$.
$C_i = V(I_j) \implies V(I_1) \supseteq V(I_2) \cdots \implies \sqrt{I_1} \subseteq \sqrt{I_2} \subseteq \sqrt{I_3} \subseteq \cdots$
R Noetherian $\implies$ this stabilises. □

Definition 2.14.8
A closed set C of a topological space X is irreducible if $C \neq C_1 \cup C_2$ for $C_1, C_2 \subsetneq C$ proper closed. ($\iff$ $C \subseteq C_1 \cup C_2$, C_1, C_2 closed subsets then $C \subseteq C_1$ or $C_2 \subseteq C_2$).

Lemma 2.14.9
X Noetherian topological space. Then any closed set of X can be expressed as a finite union $C_1 \cup C_2 \cup \cdots \cup C_n$ of irreducible closed sets $C_1, \ldots, C_n$. This is unique if $C_i \not\subseteq C_j$ $\forall i \neq j$.

Proof
Let $S = \{\text{Closed subsets of } X \text{ that cannot be expressed in this way}\}$. Want to show that $S = \emptyset$. Assume $Y_0 \in S$, then Y_0 is not irreducible. $\implies Y_0 = C_1 \cup C_2$, $C_1, C_2 \subsetneq Y_0$ closed.
Claim $C_1 \in S$ or $C_2 \in S$ (otherwise $Y_0 \notin S$). Say $C_1 \in S$. Set $Y_1 = C_1 \implies Y_0 \supsetneq Y_1$, $Y_0, Y_1 \in S$.

Repeat process $\implies Y_0 \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots$ does not stabilise. Contradiction.

Uniqueness:
If $C_1 \cup \cdots \cup C_n = C_1' \cup \cdots \cup C_n'$ with $C_i \not\subseteq C_j \; \forall i \neq j$ and $C_i' \not\subseteq C_j' \; \forall i \neq j$, then $C_i \subseteq C_1' \cup \cdots \cup C_m' \implies C_i \subseteq C_j'$ for some j.

Similarly $C_j' \subseteq C_k$ for some $k \implies C_j \subseteq C_j' \subseteq C_k \implies i = k \implies C_i = C_j'$. □

Definition 2.14.10
If $C = \underbrace{C_1 \cup \cdots \cup C_n}_{\text{irred. closed}}$ such that $C_i \not\subseteq C_j \; \forall i \neq j$, then C_i's are the irreducible components of C.
Remark: If $C = \text{Spec}(R)$, then irreducible componenets of $\text{Spec}(R)$ are the maximal irreducible closed subsets of $\text{Spec}(R)$.
If $Z \subset X$ maximal irreducible, $Z \subseteq C_1 \cup \cdots \cup C_n \implies Z \subseteq C_i \implies Z = C_i$. (maximal)

Proof of Prime ideals of $R \overset{1-1}{\longleftrightarrow}$ Irreducible closed sets in $\text{Spec}(R)$
Sufficient to prove:

1. $\mathfrak{p}$ prime $\implies V(\mathfrak{p})$ irreducible
2. $V(\sqrt{I}) = V(I)$ irreducible $\implies \sqrt{I}$ prime

Proof of 1:
$V(\mathfrak{p}) \subseteq V(I) \cup V(J)$.
Since $\mathfrak{p} \in V(\mathfrak{p})$, $\mathfrak{p} \in V(I)$ or $\mathfrak{p} \in V(J) \implies \mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J \implies V(\mathfrak{p}) \subseteq V(I)$ or $V(\mathfrak{p}) \subseteq V(J)$.

Proof of 2:
Assume $V(I) = V(\sqrt{I})$ irreducible. Let $xy \in \sqrt{I}$.
Prove $x \in \sqrt{I}$ or $x \in \sqrt{I}$. $xy \in \mathfrak{p} \; \forall \mathfrak{p}$ prime, $\mathfrak{p} \supseteq I$
$\implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$
$\implies \mathfrak{p} \in V((x)) \cup V((y))$
$\implies V((x)) \subseteq V((y))$
by irreducibility of $V(\sqrt{I}) \implies V(\sqrt{I}) \subseteq V((x))$ or $V(\sqrt{I}) \subseteq V((y))$.
Say $V(\sqrt{I}) \subseteq V((x))$, then $\sqrt{(x)} = \sqrt{\sqrt{I}} = \sqrt{I}$.
$x \in (x) \subseteq \sqrt{(x)} \implies x \in \sqrt{I}$. □

Theorem 2.14.11 Hilbert's Basis Theorem
R Noetherian $\implies R[X]$ Noetherian.

Example 2.14.12
R Noetherian $\implies R[X_1, \ldots, X_n]$ Noetherian, and all quotients $R[X_1, \ldots, X_n]/I$ Noetherian. Try $R = \mathbb{Z}, k$.
Remark: Algebraic Geometry studies $\text{Spec}(R)$, $R = k[X_1, \ldots, X_n]/I$.
Geometric Counterpart of $V(I)$ is

$$Z(I) = \{(z_1, \ldots, z_n) \in k^n \mid f_i(z_1, \ldots, z_n) = 0 \quad \forall i = 1, \ldots, n\}$$

This means for $k = \mathbb{C}$, $\exists$ 1-1 correspondence:

$$V(I) \cap \{\mathfrak{p} \text{ maximal}\} \overset{1-1}{\longleftrightarrow} Z(I)$$

2.15 Unique Factorisation Domains

Definition 2.15.1
A domain R is a Unique Factorisation Domain (UFD) if any $x \in R \setminus \{0\}$, $x = u\pi_1 \cdots \pi_n$, u a unit, π_i irreducible. If $x = v\pi_1' \cdots \pi_n'$, then $n = m$, and up to reordering, π_i, π_j' associates.

Proposition 2.15.2
In a UFD, irreducible $\iff$ prime.

Proof
($\Leftarrow$) Holds in any ring.
($\Rightarrow$) Let π be irreducible and $\pi \big| xy$
$\implies$ $\exists$ factorisation of cy with π in it, since (factorisation of x)(factorisatino of y) = factorisation of xy
$\implies$ π is associative to one element in the factorisation of x or factorisatino of y $\implies$ $\pi \big| x$ or $\pi \big| y$. $\square$

Remark: In a UFD, GCD's exists (unique up to units). GCD(f, g) = product of irreducibles common to f, g.

Proposition 2.15.3
PID $\implies$ UFD.

Proof
Let R be a PID, $x \in R \setminus \{0\}$.

Existence (This proof only uses that PID's are Noetherian)
Assume x is not a unit. If x irreducible, then done. So assume x not irreducible then $x = x_1y_1$, x_1, y_1 not units $\implies$ $(x) \subsetneq (x_1)$.
If x_1 not irreducible, $x_1 = x_2y_2$, x_2, y_2 not units, then continue with x_2, x_3 etc.
$\implies$ $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$
This must stop by Noetherian property of R.
$\implies$ one x_i is irreducible. Set $\pi_1 = x_i$, $x = \pi_1 z_1$, $z_1 \in R$. If z_1 is not a unit, then $z_1 = \pi_1 z_2$, continue with z_2 etc, then $(x) \subsetneq (z_1) \subsetneq \cdots$. Assume this must stop, i.e. at some point π_i is a unit. $x = u\pi_1 \cdots \pi_n$.

Uniqueness:
Induction on number of irreducible appearing in some factorisation of x.
Assume $x = u\pi_1 \cdots \pi_n = v\pi_1' \cdots \pi_m'$.
$\pi_n \big| \pi_1' \cdots \pi_m'$ $\implies$ ($\pi_n$prime in PID) $\pi_n \big| \pi_i'$ for some i. Say $i = m$, $\pi_n \big| \pi_m'$ $\implies$ π_n, π_m' are associates, $\pi_n = \omega\pi_m$, ω a unit $\implies$ $uw\pi_1 \cdots \pi_{n-1} = v\pi_1' \cdots \pi_{m-1}'$.
Continue by induction. $n - 1 = m - 1$ and up to reordering, $\pi_i = \pi_i'$ are associates. $\square$

Example 2.15.4
Euclidean Domains $\subset$ PID $\subset$ UFD. PID $\subset$ Noetherian rings.
GCD's computed by Euclidean algorithms, GCD$(x, y) = ax + by$, GCDs exist.
$\mathbb{Z}, k[X], \mathbb{Z}[i]$
$\mathbb{Z}[\sqrt{-5}]$ is Noetherian since $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(x^2 + 5)$ but not UFD: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Theorem 2.15.5
R UFD $\implies$ $R[X]$ UFD. (e.g. $\mathbb{Z}[X]$, $k[X,Y]$ UFDs but not PIDs)

Proposition 2.15.6
In a PID:

- Nonzero prime ideals are maximal
- $I \neq 0$ then I is contained in finitely many maximal ideals

Corollary 2.15.7
R a PID. $V(I)$ are either $\mathrm{Spec}(R)$, $\emptyset$, or $\{(\pi_1), \ldots, (\pi_n)\}$.

Proof
1. Let (x) be prime, i.e. x prime. If $(x) \subseteq (y)$, then $y \big| x \implies$ (since x prime irreducible) y is either a unit or a associate to $x \implies (y) = R$ or $(y) = (x)$
2. $I = (x) \subseteq (\pi) \implies \pi \big| x \implies \pi$ is an (associate of) an irreducible in fact of x and there are finitely many. □

Proposition 2.15.8 Gauss's Lemma
If R is a UFD and $K = \mathrm{Frac}(R)$. If $f(x) \in R[X] \subseteq K[X]$ and $f(x) = g(x)h(x)$, $g, h \in K[X]$, g, h non-constant, then $f(x)$ factors $f(x) = g'(x)h'(x)$, $g', h' \in R[X]$ g', h' non-constant.
Exercise: If $f(x)$ factors in $\mathbb{Q}[X]$ then actually it factors in $\mathbb{Z}[X]$. ($f \in \mathbb{Z}[X]$)

Proof
Coefficient of g, h are $\frac{p}{q}, p, q \in R$. Clear denominators to get $df(x) = g'(x)h'(x)$, $d \in R, g', h' \in R[X]$.

Now write $d = u\pi_1 \cdots \pi_n$ (irreducibles/primes)
If $n = 0$, done.
Otherwise consider $R[X]/(\pi_m) \cong R/(\pi_m)[X]$. (exercise)
R domain $\iff$ $R[X]$ domain.
π_n prime $\implies$ $(R/(\pi_m))[X]$ domain.

In $R[X]/(\pi_m)$,

$$0 = \overline{df(x)} = \overline{g'h'} \implies \overline{g'(x)} \text{ or } \overline{h'(x)}$$

$\implies$ π_m divides all coefficients g' or of h. Factor π_m out and continue. □

Corollary 2.15.9
GCD of coefficients of f and $g = 1$ $\iff$ GCD of coefficient of $fg = 1$.

Proof
($\Rightarrow$) Follows from proof of Gauss's Lemma
($\Leftarrow$) Clear. □

Proposition 2.15.10
If $f \in R[X]$ non-constant, then f is irreducible in $R[X]$ $\iff$ f is irreducible in $K[X]$ and GCD of coefficient of f is 1.

Proof
($\Rightarrow$) If f is reducible in $k[X]$ then f reducible in $R[X]$ by Gauss lemma. Contradiction. If GCD of coefficent of f is not 1, $f = \pi g(x)$, π irreducible in $R \implies f$ not irreducible in $R[X]$. Contradiction.

($\Leftarrow$) Assume f reducible in $R[X]$. Then $f = gh$ non-constant, $gh \in R[X]$ or $f(x) = \pi g(x)$. π irreducible in R, $g \in R[X]$. Contradiction. $\square$

Theorem 2.15.11
R UFD $\iff$ $R[X]$ UFD.

Proof
($\Leftarrow$) Clear.
($\Rightarrow$) Let $K = \text{Frac}(R)$.
Existence:
Let $f(x) \in R[X] \subseteq K[X]$, then $f = P_1 \cdots P_k$ in $K[X]$, P_i irreducible polynomials in $K[X]$.
By proof of Gauss Lemma, $f = P_1' \cdots P_k'$ in $R[X]$ with $P_i' = d_i P_i$, $d_i \in R$.
May write $P_i' = d_i P_i$ GCD of coefficients of $P_i = 1$ (new P_i). Then P_i irreducible in $R[X]$ by proposition before.
$\implies f = \underbrace{(d_1 \cdots d_k)}_{\text{in } R} P_1 \cdots P_k$.

Uniqueness:
If $f = dP_1 \cdots P_k = eQ_1 \cdots Q_l$, $d, e \in R$, $P_i, Q_i \in R[x]$ irreducible, then GCD(coeff. f)$= d = e$ so $d = e$ up to units.
$\implies P_1 \cdots P_k = uQ_1 \cdots Q_l$ in $R[X] \subseteq K[X] \implies k = l$. After possible reordering, P_i, Q_i associates in $K[X]$. $Q = \frac{a}{b} P_i \implies bQ_i = aP_i$. GCD(coeff. bQ_i)$= b = a$ up to units. $\square$