Math 110B (Algebra)
University of California, Los Angeles

Aaron Chao

Winter 2022

These are my lecture notes for Math 110B (Algebra), which is the second course in Algebra taught by Nicolle Gonzales. The textbook for this class is *Abstract Algebra: An Introduction, 3rd edition* by Hungerford.

Contents

1 Jan 3, 2022

1.1 Groups

- Algebra $\to$ study of mathematical structure.
- Rings $\leftrightarrow$ "numbers" e.g. $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Z}_p$
  2 operations $(+, \cdot)$

Question 1.1: What happens if we have only 1 operation (either $\cdot$ or $+$ but not both)? What kind of structure is this more basic setup?

Answer: Groups! It turns out groups encode the mathematical structures of the symmetries in nature.

Definition 1.2 (Group)
A group $(G, *)$ is a nonempty set with a binary operation $* : G \times G \to G$ that satisfies

1. (Closure): $a * b \in G \quad \forall a, b \in G$
2. (Associativity): $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$
3. (Identity): $\exists e \in G$ such that $e * a = a = a * e \quad \forall a \in G$
4. (Inverse): $\forall a \in G, \exists d \in G$ such that $d * a = e = a * d$

Note:

- If * is addition, we just divide * by the usual + sign. In this case

$$e = 0 \quad \text{and} \quad d = -a$$

- If the operation * is multiplication, we just divide * by the usual $\cdot$ sign. In this case

$$e = 1 \quad \text{and} \quad d = a^{-1}$$

- Be aware that sometimes * is neither.

Definition 1.3 (Abelian)
If the * operation is commutative, i.e. $a * b = b * a$, then we say that G is abelian (named after the mathematician N.H. Abel)

Definition 1.4 (Order, Finite Group vs. Infinite Group)
The order of a group G, denoted $|G|$, is the number of elements it contains (as a set).
Thus, G is a finite group if $|G| < \infty$
and G is an infinite group if $|G| = \infty$

Examples 1.5 (Examples of a group)

1. Rings where you "forget" multiplication.

   $\to (\mathbb{Z}, +)$ integers with $* = +$, $(\mathbb{R}[X], +)$, etc.

   Note: $(\mathbb{Z}, *)$ with $* = \cdot$ is not a group. Why?

Theorem 1.6
Every ring is an abelian group under addition.

Proof. $e = 0$, inverse $= -a$ for each $a \in R$. □

Fact: If $R \neq 0$ then $(R, \cdot)$ is never a group since 0 has no multiplicative inverse.

Examples 1.7 (More examples of a group)

2. Fields without zero.

Theorem 1.8
Let $\mathbb{F}^*$ denote the nonzero elements of a field $\mathbb{F}$. Then $(\mathbb{F}^*, \cdot)$ is an abelian group.

Recall: A unit in a ring R is an element $a \in R$ with a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$.

Theorem 1.9
The set of units $\mathcal{U}$ inside a ring R is a group under multiplication.

Examples 1.10 (More examples of a group cont.)

3. $\mathcal{U}_n = \{m | (m, n) = 1\} \subseteq \mathbb{Z}_n$ is also a group, but under multiplication,

   $\underline{n = 4}$ $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}, \quad \mathcal{U}_4 = \{1, 3\}$

   $(\mathbb{Z}_4, +)$ and $(\mathcal{U}_4, \cdot)$ are groups with different binary operation!

   $\underline{n = 6}$ $\quad \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, \quad \mathcal{U}_6 = \{1, 5\}$

   $(\mathcal{U}_6, \cdot)$ is a group

   - $1 \cdot 5 = 5 \pmod 6 \in \mathcal{U}_6$ (closure)
   - $1 = e$ (identity)
   - $1 \cdot 1 = 1, \quad 5 \cdot 5 = 25 \equiv 1 \pmod 6$ (inverse)
   - Associativity is clear

2 Jan 5, 2022

2.1 Groups (Cont'd)

Examples 2.1

4. $(M_{n\times m}(\mathbb{F}), +) = m \times n$ matrices over $\mathbb{F}$ under addition
   $e =$ zero matrix, inverse of a matrix $-M$

Definition 2.2 (General linear group)
Denote by $GL_n(\mathbb{F})$ the set of $n \times n$ invertible matrices under multiplication. ($\det(A) \neq 0 \quad \forall A \in GL_n$)

- Closed: $\det(A \cdot B) = \det(A) \cdot \det(B) \neq 0 \implies AB \in GL_n \quad \forall A, B \in GL_N$
- Associativity: Obvious.
- Identity: $\det(I) = 1 \neq 0 \implies I \in GL_n(\mathbb{F})$
- Inverse: $A \in GL_n; \det(A^{-1}) = \frac{1}{\det(A)} \neq 0 \implies A^{-1} \in GL_n(\mathbb{F})$

Fact: $GL_n(\mathbb{F})$ is a group for any field $\mathbb{F}$.
Comment:

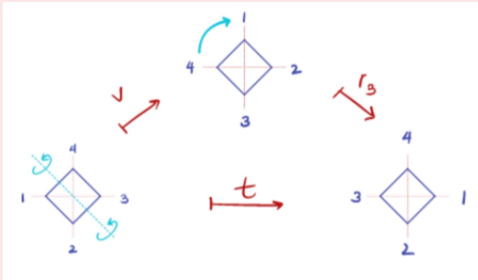
- $\det(A + B) \neq \det(A) + \det(B)$
- $\det(AB) = \det(A) \cdot \det(B)$

Definition 2.3 (Special linear group)
Let $SL_n(\mathbb{F})$ denote the set of invertible matrices over $\mathbb{F}$ with $\det = 1$

Exercise. Show that $SL_n(\mathbb{F})$ is a group.

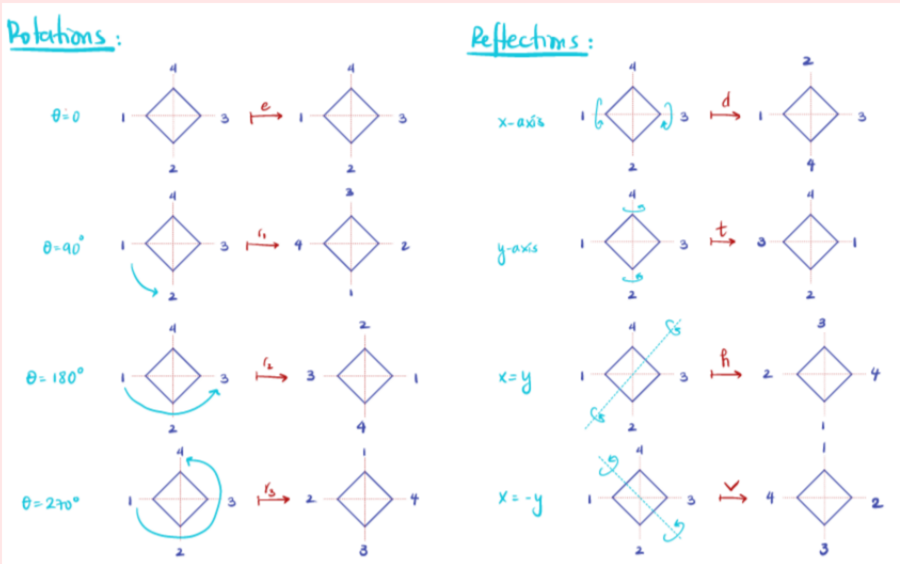
2.2 Symmetries

Example 2.4 (Symmetries over a square)
Rotations and reflection These operations (maps) form a group under composition. So $* = 0$. For instance, suppose
$r_3 \circ t = h$



The group of rotations/reflections of a square is called Dihedral Group of degree 4, denoted D_4.

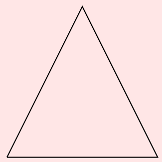
$$D_4 = \{r_1, r_2, r_3, r_4, d, t, h, v \mid \text{under } \circ\}$$



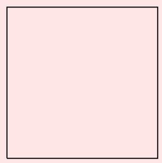
These are Professor Gonzales's lovely drawings.

Example 2.5 (Symmetries of a regular polygon with n sides)
Called the dihedral groups of degree n, D_n.

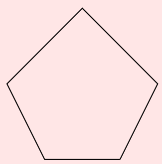
- n=3



- n=4



- n=5



- n=6

  etc...

Observe: $|D_n| = 2n$ because you have n-axes of reflection and n-angles of notation.

Example 2.6 (The symmetric group)
Let $n \in N$, and S_n be the set of all permutations of the numbers $\{1, ..., n\}$.
Note: any permutation of $\{1, ..., n\}$ can be thought of as a bijection $\{1, ..., n\} \to \{1, ..., n\}$.
$\implies$ This allows us to compose permutations just like functions.
$\implies$ S_n is a group!

Definition 2.7 (Symmetric group)
The symmetric group S_n is the group of permutations of the integers of the integers $\{1, ..., n\}$.
Given any permutation $\sigma \in S_n$,

$$\begin{aligned} \sigma : &\{1, ..., n\} \to \{1, ..., n\}, \\ &i \mapsto \sigma_i \end{aligned}$$

$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_{n-1} & \sigma_n \end{pmatrix} \to e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$
$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1^{-1} & \sigma_2^{-1} & \cdots & \sigma_n^{-1} \end{pmatrix}$

Group operation: function composition.

Example 2.8
n=2:

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\tau \circ \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e$$

$\tau \circ e = \tau$
$e \circ \tau = \tau$
$e \circ \tau = e$
$\implies S_2 = \{e, \tau\}$ is a group
$e^{-1} = e$
$\tau^{-1} = \tau$
Associativity: obvious because of function composition

3 Jan 7, 2022

3.1 Symmetries (Cont'd)

Example 3.1
n=3 S_3: permutations of $\{1, 2, 3\}$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\tau_{21} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tau_{121} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

So,

$$\begin{aligned} \tau_1 \circ \tau_2 \circ \tau_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_{121} \end{aligned}$$

Note: $\tau_{21} = \tau_2 \circ \tau_1$, $\tau_{12} = \tau_1 \circ \tau_2$
$\tau_{21} \neq \tau_{12} \implies S_3$ is not abelian!

Exercise. τ_{212}?

3.2 Direct Product of Groups

Definition 3.2 (Direct product)
Given $(G, *), (H, \star)$ both groups define the binary operation:

$$\begin{aligned} \square \colon (G \times H) \times (G \times H) &\to G \times H \\ (g, h) \,\square\, (g', h') &\mapsto (g * g', h \star h') \end{aligned}$$

Side note: $(S, ☺)$
$☺\colon S \times S \to S \implies S$ group

Example 3.3
$S_2 \times D_4$:
$(\tau_1, r_{270^\circ}) \,\square\, (\tau_1, v) = (\tau_1 \circ \tau_1, r_{270^\circ} v) = (e, t)$

Example 3.4
$(\mathbb{R}, +) \times (\mathbb{R}^*, \cdot)$
$(5, 2) \,\square\, (-5, \pi) = (0, 2\pi)$

Example 3.5
$\mathbb{Z}_n \times \mathbb{Z}_m \quad n, m \in \mathbb{N}$.
$(a, b) \,\square\, (a', b') = (\underbrace{a + a'}_{\text{mod } n}, \underbrace{b + b'}_{\text{mod } m})$

$$(5,5) \overset{\mathbb{Z}_8 \times \mathbb{Z}_6}{\square} (2,2) = (5+2, 5+2)$$
$$= (7,1)$$

3.3 Properties of Groups

Notation: Going forward, we omit $*$ in the notation: $(G, *) \to G$. Use multiplicative notation for abstract groups. Instead $a * b \to ab$.

$$\underbrace{a * a * a * a \cdots * a}_{n \text{ times}} \to a^n$$

However, for very explicit groups like
$(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Z}_n, +)$, etc, we use additive notation. $(* = +)$

$$a * b \to a + b$$

$$\underbrace{a * \cdots * a}_{n \text{ times}} \to n \cdot a$$

(Review notation on page 198 of book)

Theorem 3.6
G group, $a, b, c \in G$. Then

1. $e \in G$ is unique
2. if $ab = ac$ or $ba = ca \implies b = c$
3. $\forall a \in G : a^{-1}$ is unique.

Proof.

1. Suppose $\exists e' \in G$ s.t $e \neq e'$ but $e'a = a = ae'$ $\forall a \in G$. $\implies$ let $a = e \implies e'e = e = ee'$

   On the other hand $e \cdot e' = e' = e'e$

   $\implies e = e'$

2. $ab = ac, \quad a, b, c \in G$.

   Since $a^{-1} \in G$

$$\implies \underbrace{a^{-1}a}_{e} b = \underbrace{a^{-1}a}_{e} c$$
$$\implies e \cdot b = e \cdot c$$
$$\implies b = c$$

3. Suppose $a \in G$ $\exists$ two distinct inverses.

   $d_1, d_2 \in G$.

   $d_1 a = e = a d_1$

   $d_2 a = e = a d_2$

   $\implies d_1 = d_1 e = d_1 a d_2 = e \cdot d_2 = d_2$

□

Corollary 3.7
G group, $a, b \in G$. Then

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

Proof. Exercise. □

Note: $ab = ba$ (G is abelian)

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

Generally: $ab \neq ba \implies a^{-1}b^{-1} \neq b^{-1}a^{-1}$

3.4 Order of an Element

Definition 3.8 (Order (of an element) and Finite vs. Infinite order)
The order of an element $a \in G$ is the smallest $k \in \mathbb{N}$ such that $a^k = e$. We denote this by $|a|$.
If k is finite $\implies a$ has finite order.
If k is infinite $\implies a$ has infinite order.

Example 3.9
S_2; $e, \tau_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
Notice,

$$|e| = 1; e^1 = e$$

$$|\tau_1| = 2 \quad \tau_1^2 = \tau_1 \circ \tau_1 = e$$

$$\tau_1^4 = \tau_1^2 \circ \tau_1^2 = e \circ e = e$$

Example 3.10

$\mathbb{Z} \leftarrow e = 0$.

$|1| = ?$

$1 \cdot n = 0$ for which n?

None, so $\implies |1| = \infty$

4 Jan 10, 2022

4.1 Order of an Element (Cont'd)

Theorem 4.1
G-group, $a \in G$

1. If $|a| = \infty$, then $a^i \neq a^j$ for any $i, j \in \mathbb{Z}$ with $i \neq j$.
2. If $\exists i \neq j$ such that $a^i = a^j \implies |a| < \infty$.

Proof. We prove (2) (because $1 \iff 2$).
WLOG suppose $i > j$, then if $a^i = a^j \implies a^{i-j} = a^i a^{-j} \implies = a^j a^{-j} = a^0 = e$
$\implies |a| \leq i - j < \infty$ □

Theorem 4.2
G group, $a \in G \quad |a| = n$

1. $a^k = e \iff n \mid k \quad (n \leq k)$
2. $a^i = a^j \iff i \equiv j \pmod{n}$
3. if $n = td \quad d \geq 1 \implies |a^t| = d$.

Proof.

1. If $a^k = e$ and since $a^n = e$ with n-smallest such integer, then $k > n$, and so $k = nd + r$ with $0 \leq r < n$
$$a^k = a^{nd+r} = (a^n)^d a^r = e^d a^r = a^r$$
If $0 < r < n \implies a^r \neq e \implies a^k \neq e$
$\implies r = 0 \implies k = nd \implies n \mid k$.
2. If $a^i = a^j \implies a^{i-j} = e$
$\implies n \mid i - j$ by (1).
$\implies i - j \equiv 0 \pmod{n}$
$\implies i \equiv j \pmod{n}$
3. If $n = td\ (d \geq 1) \overset{?}{\implies} |a^t| = d$
Since $a^n = e \implies (a^t)^d = e \implies |a^t| \leq d$.
If $|a^t| = k < d \implies (a^t)^k = a^{tk} = e$
But $tk < td = n \implies a^{tk} = e$ for $tk < n \implies \neq$ because n is the smallest positive integer such that $a^n = e$.
$\implies k = d \implies |a^t| = d$.

□

Corollary 4.3
G- abelian group with $|a| < \infty \quad \forall a \in G$. Suppose $c \in G$ such that $|a| \leq |c| \quad \forall a \in G$. Then $|a| \mid |c|$.

Proof. Suppose not. $\exists$ some $a \in G$ such that $|a| \nmid |c|$. Consider prime factorizations of $|a|$ and $|c|$.
$\implies$ Then $\exists$ some prime p such that $|a| = p^r m \quad |c| = p^s n$ where $r > s$ (s might be zero) and $(p_1 m) = 1 = (p_1 n)$.
Then by (3) of Theorem 4.2,

$$|a^m| = p^r \quad \text{and} \quad |c^{p^s}| = n$$

$$\underset{\text{because } (p^r,n)=1}{\implies} |\underbrace{a^m \cdot c^{p^s}}_{\in G}| = p^r \cdot n$$

Note: $|a| = n, |b| = m, |a \cdot b| \neq n \cdot m$ unless $(n, m) = 1$
Recall: $|c| = p^s \cdot n$ where $s < r$
$\implies p^r > p^s$
$\implies p^r n > p^s n$
$\implies |a^m \cdot c^{p^s}| > |c|$
$\implies \neq$ because c is the element in G with maximal order! So $a^m c^{p^s} \in G$ cannot have order larger than c. $\square$

4.2 Subgroups

Definition 4.4 (Subgroup)
A subset $H \subseteq G$ is a subgroup of $(G, *)$ if it is also a group under $*$.
Note:
$G \subseteq G \implies G$ is always a subgroup of itself (Improper subgroup)
$\{e\} \subseteq G \implies \{e\}$ is always a subgroup of G (Trivial subgroup of G)
$\implies$ Any subgroup $e \neq H \neq G$ is called a nontrivial proper subgroup.

Examples 4.5

- $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +)$
- $\{e, r_{90}, r_{180}, r_{270}\} \subseteq D_4$
- $SL_n(\mathbb{F}) \subseteq GL_n(\mathbb{F})$

Note: any subgroup always contains e.

Theorem 4.6
A nonempty subset H of G is a subgroup if:

1. $ab \in H \quad \forall a, b \in H$
2. $a^{-1} \in H \quad \forall a \in H$

Proof. Since $H \neq \emptyset \quad \exists a \in H$. By (2), $\exists a^{-1} \in H$. $\implies$ By (1) $aa^{-1} = e \in H \implies e \in H$. $\square$

Theorem 4.7
Any closed nonempty finite subset H of G is a subgroup.

Proof. By Theorem 4.6, we need only show that H contains inverses.
If $a \in H \quad a^k \in H \quad \forall k \in \mathbb{Z}$.
Since H is finite, not all a^k can be distinct.
$\implies |a| = n < \infty$ for some $n \in \mathbb{N}$.
$\implies a^n = e$
$\implies a^{n-1} \cdot a = e = a \cdot a^{n-1}$
$\implies a^{n-1} = a^{-1}$
If $n > 1 \implies a^{-1} \in H$
If $n = 1 \implies a^{-1} = e \implies a = e \implies a^{-1} = e \in H$. $\square$

5 Jan 12, 2022

5.1 Subgroups (Cont'd)

Example 5.1
$\mathbb{Z}_5 \leftarrow$ group under addition $= \{0, 1, 2, 3, 4\}$
Units of $\mathbb{Z}_5$: $\mathcal{U}_5 = \{1, 2, 3, 4\}$
Clearly, $\mathcal{U}_5 \subseteq \mathbb{Z}_5$
Question: Is $\mathcal{U}_5$ a subgroup of $\mathbb{Z}_5$
No, because $\mathcal{U}_5$ is a group under multiplication.

Example 5.2
S_3: set of permutations that fix 1.
$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$$\left.\begin{array}{l} \tau_2 e = \tau_2 = e\tau_2 \\ \tau_2 \cdot \tau_2 = e \end{array}\right\} \implies \underbrace{\{e, \tau_2\}}_{H} \text{ is closed.}$$

By Theorem 4.7, H is a subgroup because H is finite, nonempty, and closed.

5.2 Center of a Group

Definition 5.3 (Center of a group)
The <u>center</u> of a group G is the subset

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

Note 5.4: When G is abelian $\implies Z(G) = G$

Question 5.5: Is $Z(G) = \emptyset$? No, because $e \in Z(G)$

Examples 5.6

- $Z(S_n) = e$
- $Z(D_4) = \{e, r_{180}\}$
- $Z(GL_n) = \{aI \mid a \in \mathbb{F}\} \qquad \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$
- $Z(SL_n) = \{I\} = e$

Theorem 5.7
$Z(G)$ is a subgroup of G.

Proof. By Theorem 4.6, since $Z(G) \neq \emptyset$, we need only show closure and inverses.

1. $a, b \in Z(G) \overset{?}{\implies} ab \in Z(G), \forall g \in G.$
   $(ab)g \overset{\text{b/c } g \in Z(G)}{=} a(gb) \underset{\text{by assoc.}}{=} (ag)b \overset{a \in Z(G)}{=} (ga)b = g(ab)$
   $\implies ab \in Z(G)$
2. $a \in Z(G), ag = ga \quad \forall g \in G.$
   $\implies a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$
   $\implies ga^{-1} = a^{-1}g \implies a^{-1} \in Z(G)$

$\square$

5.3 Cyclic Group

Definition 5.8 (Cyclic group)
For any $a \in G$, the set

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G. We say $\langle a \rangle$ is the cyclic subgroup generated by a.

Note 5.9: Cyclic groups are always abelian.

If $G = \langle a \rangle$ for some $a \in G$, then G is a cyclic group.

Example 5.10
$\langle r_{90} \rangle \subseteq D_4$
$\langle r_{90} \rangle = \{e, r_{90}, r_{180}, r_{270}\} \leftarrow$ is a cyclic subgroup of G.

Note 5.11: In additive notation: $a * a = a + a$ (not $a \cdot a = a^2$)

$$\langle a \rangle = \{n \cdot a \mid n \in \mathbb{Z}\} \quad n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

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

Example 5.12
$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

Note 5.13: The generating element a is not unique.

Example 5.14
$(\mathbb{Z}_3, +) = \langle 1 \rangle = \underset{=-1}{\langle 2 \rangle}$

Exercise. Which elements generate $\mathbb{Z}_n$ for $n \in \mathbb{N}$?
Hint: Look at units (i.e. relatively prime) of $\mathbb{Z}_n$

Example 5.15
$\mathbb{Z}_n = \langle 1 \rangle$
$\implies$ All $\mathbb{Z}_n$ are cyclic groups of order n

Theorem 5.16
Let $a \in G$

1. If $|a| = \infty$, then $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is an infinite group.
2. If $|a| = n < \infty$, then $\langle a \rangle$ is a finite group. In fact, $\langle a \rangle = \langle e, a, a^2, a^3, \ldots, a^{n-1}\} \implies |\langle a \rangle| = |a| = n$.

Proof (Sketch).

$$\begin{aligned} |a| = \infty &\implies a^i \neq a^j \text{ for } i \neq j \\ &\implies \{a^k \mid k \in \mathbb{Z}\} \implies \text{ infinite set.} \\ |a| = n &\implies \langle a, a^2, \ldots, a^{n-1}, a^n = e\} \end{aligned}$$

Since: $a \cdot a^{n-1} = a^n = e = a^{n-1} \cdot a$

$$\implies a^{n-1} = a^{-1}$$

$a^2 a^{n-2} = a^n = e = a^{n-2} a^2$

$$\implies a^{-2} = a^{n-2}$$

□

Theorem 5.17
Let $\mathbb{F}$ be any field. Then any finite subgroup $G \subseteq \mathbb{F}^*$ is cyclic.

Recall 5.18 $\mathbb{F}^* = \mathbb{F} - \{0\}$ is a group under multiplication.

Proof. Since $|G| < \infty$, $\exists c \in G$ such that order of c is maximal ($|a| \leq |c| \quad \forall a \in G$). By Corollary 4.3, $\forall a \in G, |a| \mid |c|$ so if $|c| = m \implies a^m = 1$
Consider $p(x) = x^m - 1$. Since $p(a) = 0 \quad \forall a \in G$.
Since $p(x)$ has degree m it can have at most m solutions $\implies |G| \leq m$.
Since $|c| = m$ so $|\langle c \rangle| = m$.
$\implies \langle c \rangle \subseteq G \implies \langle c \rangle = G$.
$\implies G$ is cyclic. □

6 Jan 14, 2022

6.1 Cyclic Group (Cont'd)

Recall 6.1 $a \in G$

$$\underbrace{\langle a \rangle}_{\text{cyclic group gen. by a}} := \{a^n \mid n \in \mathbb{Z}\} = \{\dots a^{-2}, a^{-1}, e, a, a^2, \dots\}$$

$G = \langle a \rangle \leftarrow G$ is cyclic group

Recall 6.2 Thm:

$$|a| = \infty \to |\langle a \rangle| = \infty$$
$$|a| = n < \infty \to |\langle a \rangle| = n$$

Recall 6.3 $\mathbb{F}$-field, $G \subseteq \mathbb{F}^*$ if G finite $\implies$ G is cyclic. (G is any subgroup)

Theorem 6.4
Subgroups of cyclic groups are cyclic.

Proof. Suppose $G = \langle a \rangle$ and $H \subseteq G$. We want to show that $H = \underbrace{\langle b \rangle}_{b=a^j \text{ for some } j}$ for some $b \in G$.

If $H = e \implies H = \langle e \rangle$ we're done.
If $H \neq e$, then we can find k-smallest positive integer such that $a^k \in H$
Suppose $b \in H$. Then,

$$b = a^i \text{ for some } i \text{ then } i = kd + r \quad 0 \leq r < k.$$

$\implies a^r = a^{i-kd} = b(a^k)^{-d} \in H$ by closure.
If

$$r \neq 0 \implies \begin{cases} a^r \in H \\ a^k \in H \end{cases}$$

with $0 < r < k$ which is a contradiction because k was supposed to be smallest positive integer with $a^k \in H$.

$$\begin{aligned} \implies r = 0 &\implies b = a^i = a^{kd+r} = a^{kd} = (a^k)^d \\ &\implies b \in \langle a^k \rangle \\ &\implies H \subseteq \langle a^k \rangle \end{aligned}$$

$$\begin{aligned} \text{Since } a^k \in H &\implies \langle a^k \rangle \subseteq H \\ &\implies \langle a^k \rangle = H \end{aligned}$$

$\square$

6.2 Generating Sets for Groups

Definition 6.5
Given a subset S of G, let $\langle S \rangle$ denote the set of all possible products of all elements of S and their inverses.

Note 6.6: $S \subseteq \langle S \rangle$

Example 6.7
$a, b \in G, \quad S = \{a, b\}$

$$\begin{aligned}
\langle S \rangle &= \langle a, b \rangle \\
&= \{a^n, b^m, a^n b^m, a^{n_1} b^{m_1} a^{n_2} b^{m_2}, b^m a^n, b^{m_1} a^{n_2} b^{m_2} a^{n_1}, \dots\} \\
&= \left\{ \prod_{i=0}^{k} a^{n_i} b^{m_i}, \prod_{i=0}^{k} b^{n_i} a^{m_i} \mid k \in \mathbb{N}, n_i, m_i \in \mathbb{Z} \right\}
\end{aligned}$$

Theorem 6.8
S- any subset of G.

1. $\langle S \rangle$ is always a subgroup of G.
2. If H is any other subgroup of G such that $S \subseteq H \implies \langle S \rangle \subseteq H$.

Proof (Sketch).

1. Use the fact that very definition of $\langle S \rangle$ ensures closure and inverses $\implies \langle S \rangle$ is a subgroup.
2. Again follows from closure and inverses contained in H because H is a subgroup.

$\square$

Definition 6.9 (Generators)
For any $S \subseteq G$, the group $\langle S \rangle$ is called the subgroup generated by S. If $G = \langle S \rangle$, then we call elements in S, the generators of G and S the generating set of G

Example 6.10 (Symmetric group)
$S_3 = \{e, \tau_1, \tau_2, \tau_{121}, \tau_{21}, \tau_{12}\}$
$\tau_{121} = \tau_1 \circ \tau_2 \circ \tau_1$
$\tau_{21} = \tau_2 \circ \tau_1$
$\tau_{12} = \tau_1 \circ \tau_2$
$e = \tau_1 \circ \tau_1 = \tau_2 \circ \tau_2$

$$S_3 = \langle \overbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}^{\tau_1}, \overbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}^{\tau_2} \rangle$$

$S_n \leftarrow$ order $n!$

$$S_n = \langle \underbrace{\tau_1}_{\text{flips } 1-2}, \underbrace{\tau_2}_{2-3}, \tau_3, \ldots, \underbrace{\tau_{n-1}}_{\text{flips } n, n-1} \rangle$$

$S_4 = \langle \tau_1, \tau_2, \tau_3 \rangle$
$S_5 = \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle$

6.3 Isomorphisms and Homomorphisms

Definition 6.11 (Homomorphism (of groups))
G, H are groups. A homomorphism of groups is a map $\varphi \colon G \to H$ such that $\forall a, b \in G$

$$\varphi(\underbrace{ab}_{ab \text{ prod in } G}) = \varphi(a) \underbrace{\cdot}_{\text{prod in } H} \varphi(b)$$

Note 6.12: This means that the "multiplication" table for G is mapped onto "multiplication" table for H i.e. φ preserves group structures.

Note 6.13: $\varphi(a) = \varphi(e_G \cdot a) = \varphi(e_G)\varphi(a)$
$\implies \varphi(e_G) = e_H$
$\implies \varphi$ takes identities to identities.

Definition 6.14 (Isomorphism (of groups))
An isomorphism of groups G and H is a homomorphism of $\varphi \colon G \to H$ that is also a bijection, i.e. an isomorphism is an invertible homomorphism.
If G is isomorphic to H, then $G \cong H$, which is the same as writing $\exists \varphi \colon G \to H$ with φ one-to-one and onto. Alternatively, $\tilde{\varphi} \colon H \to G$ is also one-to-one and onto.

Example 6.15
$\mathbb{Z}_8 = \{0, \dots, 7\}$
$\mathcal{U}_8$ of units $\implies \mathcal{U}_8 = \{\underset{e=}{1}, 3, 5, 7\}$
Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\underset{e=}{(0,0)}, (1,0), (0,1), (1,1)\}$
Claim: $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathcal{U}_8$
Let

$$\begin{aligned} \varphi \colon \mathcal{U}_8 &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \varphi(1) &= (0,0) \\ \varphi(3) &= (1,0) \\ \varphi(5) &= (0,1) \\ \varphi(7) &= (1,1) \end{aligned}$$

$\varphi(ab) = \varphi(a) + \varphi(b)$
Check,

- φ is a homomorphism
- multiplication table is preserved
- φ is one to one and onto

7 Jan 19, 2022

7.1 Isomorphisms and Homomorphisms (Cont'd)

Example 7.1 (Example 6.15 Cont'd)
Let

$$\begin{aligned} \varphi \colon \mathcal{U}_8 &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \varphi(1) &= (0,0) \leftarrow \text{ fixed} \\ \varphi(3) &= (1,0) \\ \varphi(5) &= (0,1) \\ \varphi(7) &= (1,1) \end{aligned}$$

Check,

$$\begin{aligned} (0,0)+(1,0) = \varphi(1)+\varphi(3) &\overset{\checkmark}{=} \varphi(1\cdot 3) = \varphi(3) = (1,0) \\ (0,0) = 2(0,1) = \varphi(5)+\varphi(5) &\overset{\checkmark}{=} \varphi(5\cdot 5) = \varphi(1) = (0,0) \\ &\vdots \end{aligned}$$

Verify every time $\varphi(ab) = \varphi(a)+\varphi(b) \implies \varphi$ is a homomorphism.
φ is one-to-one and onto $\implies$ DONE.
Iso's are not unique. In fact,

$$\begin{aligned} \varphi(1) &= (0,0) \\ \varphi(3) &= (0,1) \\ \varphi(5) &= (1,0) \\ \varphi(7) &= (1,1) \end{aligned}$$

is also an iso. However,

$$\begin{aligned} \varphi(1) &= (0,0) \\ \varphi(3) &= (1,1) \end{aligned}$$

Does it work? Why? (Exercise)

Example 7.2
$\mathbb{Z} \to Z_5$

$n \overset{\varphi}{\mapsto} [n] \mod 5$
Let's construct a homomorphism.

1. Check φ is well defined.

   $n \equiv m \mod 5 \overset{?}{\implies} \varphi(n) = \varphi(m).\checkmark$

2. φ is a homomorphism.

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$[a+b] \underset{\text{true}}{=} [a] + [b]$$
$$\implies \varphi \text{ is a homomorphism}$$

   Note: φ is not injective because $|\mathbb{Z}| > |\mathbb{Z}_5|$

   φ is not an iso.

Fact 7.3: Isomorphic groups always have the same order.
Converse? $|G| = |H| \implies G \cong H$?
FALSE!

Example 7.4
Consider S_3 and $\mathbb{Z}_6$.

$$|S_3| = 3! = 6 \qquad\qquad |\mathbb{Z}_6| = 6$$

Not isomorphic. Let's suppose $\varphi\colon S_3 \to \mathbb{Z}_6$ an isomorphism.

$$\varphi(ab) = \varphi(a) + \varphi(b) \tag{1}$$

So,

$$\begin{aligned} \varphi(a) + \varphi(b) &= \varphi(b) + \varphi(a) && \text{(because } \mathbb{Z}_6 \text{ is abelian)} \\ &= \varphi(ab) \end{aligned}$$

$\implies$ if (1) holds since $\mathbb{Z}_6$ is abelian
$\implies \varphi(ab) = \varphi(ba) \quad \forall b, a \in S_3$
$\implies S_3$ is abelian
False, S_3 is not abelian, so you can't define such an iso φ.

Theorem 7.5
If G is abelian, H is not abelian $\implies G \ncong H$.

Fact 7.6: Isomorphisms preserve order of elements, i.e.

$$|a| = |\varphi(a)|$$

Definition 7.7 (Automorphism)
An automorphism is an isomorphism from $G \to G$. They capture internal symmetries of a group.

Example 7.8
identity:

$$\begin{aligned} i_G \colon G &\to G \\ g &\mapsto g \end{aligned}$$

Clearly: $i(ab) = i(a)i(b) = ab \stackrel{\checkmark}{=} ab$

Definition 7.9 (Inner automorphism of G induced by c)
For any $c \in G$, the inner automorphism of G induced by c is:

$$\varphi_c \colon G \to G; \quad \varphi_c(g) = c^{-1}gc \leftarrow \text{ conjugation by } c.$$

1. Then φ_c is a homomorphism:
   $\varphi_c(ab) = c^{-1}abc = (c^{-1}ac)(c^{-1}bc) = \varphi_c(a)\varphi_c(b)$
2. φ is surjective: Given any $g \in G$.
   $\varphi_c(cgc^{-1}) = c^{-1}(cgc^{-1})c = g$
3. φ is injective: $\varphi_c(a) = \varphi_c(b)$ for some $a, b \in G$
   $\implies c^{-1}ac = c^{-1}bc$
   $\implies a = b$
   $\implies \varphi$ is an isomorphism.

7.2 Classification of Cyclic Groups

Theorem 7.10
Suppose G is a cyclic group.

1. $|G| = \infty \implies G \cong (\mathbb{Z}, +)$
2. $|G| = n < \infty \implies G \cong (\mathbb{Z}_n, +)$

Proof.

1. If $G = \langle a \rangle$ infinite. Then $G = \{a^n \mid n \in \mathbb{Z}\}$. So let

$$\begin{aligned} \varphi \colon G &\to \mathbb{Z} \\ a^n &\mapsto n \end{aligned}$$

   So φ is one-to-one and onto by definition.

Then,

$$n + m = \varphi(a^{n+m}) = \varphi(a^n a^m) \stackrel{?}{=} \varphi(a^n) + \varphi(a^m) = n + m$$

$\implies \varphi$ is a homomorphism and φ is bijection.

$\implies \varphi$ is an isomorphism.

2. $|G| = n \implies G = \{e, a, a^2, \ldots, a^{n-1}\}$

$$\begin{aligned} \varphi \colon G &\to \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \\ a^i &\mapsto i \end{aligned}$$

Exactly for the same reasons: check φ is an isomorphism.

$$k = \underbrace{\varphi(a^k)}_{i+j \equiv k \mod n} = \varphi(a^{i+j}) = \underbrace{\varphi(a^i) + \varphi(a^j)}_{i+j \equiv k \mod n}$$

φ is an isomorphism.

$\square$

8 Jan 21, 2022

8.1 Homomorphisms

Recall 8.1 Let $\varphi\colon G \to H$ any map. Then

$$\operatorname{Im}\varphi = \{h \in H \mid h = \varphi(g) \text{ some } g \in G\}$$

Theorem 8.2
If $\varphi\colon G \to H$ is a homomorphism, then:

1. $\varphi(e_G) = e_H$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. $\operatorname{Im}\varphi$ is a subgroup of H
4. If φ is injective, then $G \cong \operatorname{Im}\varphi$

Note 8.3: If φ is surjective, then $\operatorname{Im}\varphi = H$

Proof.

1. Did before.
2. By (1), $e_H = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\cdot\varphi(a^{-1}) \stackrel{?}{=} e_H \stackrel{?}{=} \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_H$ by (1).
3. Claim $\operatorname{Im}\varphi$ subgroup of H. Since $\varphi(e_G) = e_H$ by (1) $\implies e_H \in \operatorname{Im}\varphi$. If $a, b \in \operatorname{Im}\varphi \implies \exists\, a', b' \in G$ s.t. $\varphi(a') = a, \varphi(b') = b \implies ab = \varphi(a')\varphi(b') = \varphi(a'b')$ since G is closed, $a'b' \in G \implies ab \in \operatorname{Im}\varphi \implies \operatorname{Im}\varphi$ is closed.
4. By (2), if $\varphi(g) = a$ then
$$a^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$$
$\implies a^{-1} = \varphi(g^{-1})$ but $g^{-1} \in G \implies a^{-1} \in \operatorname{Im}\varphi$

   $\operatorname{Im}\varphi$ has inverses $\implies \operatorname{Im}\varphi$ is subgroup.
5. φ injective $\implies G \cong \operatorname{Im}\varphi$. Since $\varphi\colon G \to \operatorname{Im}\varphi$ is surjective by construction, if φ is also injective, then $\varphi\colon G \to \operatorname{Im}\varphi$ is a bijection and a homomorphism $\implies \varphi\colon G \to \operatorname{Im}\varphi$ is an isomorphism $\implies G \cong \operatorname{Im}\varphi$.

$\square$

Example 8.4
$\varphi\colon G \to H$ where φ is an injective homomorphism and H is abelian.
Question: Is G abelian?
Yes, because $G \cong \operatorname{Im}\varphi$ by bijectivity, and $\operatorname{Im}\varphi$ subgroup of H and subgroups of abelian groups are abelian $\implies$ G has to be abelian.

8.2 Congruence

Definition 8.5 (Congruence of a group)
Suppose H is a subgroup of G. Let $a, b \in G$. We say $a \equiv b \pmod H$ if $ab^{-1} \in H$.

Recall 8.6 An equivalence relation on a set S is a relation $a \sim b$ for $a, b \in S$ that is:
reflexive: $a \sim a \quad \forall a \in S$
transitive: $a \sim b$ and $b \sim c \implies a \sim c$
symmetric: $a \sim b \implies b \sim a$.

Theorem 8.7
The congruence relation $a \equiv b \pmod H$ is an equivalence relation for any subgroup $H \subseteq G$.

Definition 8.8 (Right coset (and left coset))
Given any $a \in G$, the right coset of H in G is:

$$Ha = \{ha \in G \mid h \in H\} \text{ where } a \text{ is any } a \in G \text{ fixed}$$

This is a right coset because a is multiplied on the right.
The left coset of H in G is:

$$aH = \{ah \in G \mid h \in H\} \text{ where } a \text{ is any } a \in G \text{ fixed}$$

Note 8.9: Ha is just the congruence class of a in $G \mod H$.
For any $a \in G$,

$$\begin{aligned}
[a] &= \{b \in G \mid b \equiv a \mod H\} \\
&= \{b \in G \mid ba^{-1} \in H\} \\
&= \{b \in G \mid \underbrace{ba^{-1} = h}_{b = ha} \text{ for some } h \in H\} \\
&= \{ha \in G \mid h \in H\} = Ha.
\end{aligned}$$

Theorem 8.10
1. $Ha = Hb$ iff $ab^{-1} \in H$ (i.e. $a \equiv b \mod H$)
2. Given $a \neq b$ either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.

Proof. Analogous as for rings (seen this in 110A). $\square$

8.3 Lagrange's Theorem

Theorem 8.11
H-subgroup of G then:

1. $G = \bigcup_{a \in G} Ha$
2. $\forall a \in G, \exists$ bijection between $H \to Ha$. So if $|H| < \infty$, then $|Ha| = |Hb| \, \forall a, b \in G$.

Proof.

1. $\bigcup_{a \in G} Ha \subseteq G$ obvious. Given $g \in G, g = eg$ where since $e \in H \implies eg \in Hg \implies g \in Hg \implies G \subseteq \bigcup_{g \in G} Hg$
2. Consider

$$\begin{aligned} \psi \colon H &\to Ha = \{ha \mid h \in H\} \\ h &\mapsto ha \end{aligned}$$

ψ is surjective by definition. If $\psi(h) = \psi(h') \implies ha = h'a \implies h = h' \implies \psi$ is injective $\implies \psi$ is a bijection.

$\square$

Definition 8.12 (Index)
Given any subgroup H of G, the <u>index of H in G</u> denoted $[G:H]$ is the number of distinct right cosets of H in G.

Theorem 8.13 (Lagrange's Theorem)
If $H \subseteq G$ is a finite subgroup, then:

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

9 Jan 24, 2022

9.1 Lagrange's Theorem (Cont'd)

Proof of Lagrange's Theorem. Suppose $[G:H] = n$ and denote the cosets by Hg_i for $i = 1, \ldots, n$.
Recall: $Hg_i \cap Hg_j = \emptyset \quad i \neq j$, also

$$G = \bigcup_{i=1}^{n} Hg_i = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n$$

$$\implies |G| = |Hg_1| + |Hg_2| + \cdots + |Hg_n|$$

Also know by previous theorem $|Hg_i| = |H| < \infty$

$$\implies |G| = n \cdot |H|$$
$$\implies \frac{|G|}{|H|} = n = [G:H]$$

□

Question 9.1: What fails when $|H| = \infty$?

Example 9.2
$n\mathbb{Z} = \langle n \rangle$ inside $\mathbb{Z}$.
Then for $a \in \mathbb{Z}$,

$$[a] = \underbrace{a + n\mathbb{Z}}_{Ha} = \{a + ni \mid i \in \mathbb{Z}\} = \{a, a+n, a+2n, \ldots\}$$

where $Ha = \{ha \mid h \in H\}$ with $H = n\mathbb{Z} \to Ha = Hb \iff ab^{-1} \in H$ and $a \equiv b \mod H$

$$a + n\mathbb{Z} = \underbrace{(a+n)}_{b} + n\mathbb{Z}$$

$-n = a-(a+n) \in n\mathbb{Z} \iff a \equiv a+n \pmod{n} \implies$ exist exactly n cosets $[0], [1], \ldots, [n-1]$

$$[\mathbb{Z}:n\mathbb{Z}] = n$$

Lagrange's Theorem $\implies |H|$ divides $|G|$ for any H subgroup of G.

Example 9.3
If G has order 15.
G can only have subgroups of orders 1, 3, 5, 15.

Note 9.4: Lagrange does not imply that subgroups exist for every number dividing $|G|$. In Example 9.3, there may not exist a subgroup of order 5 or 3.

Corollary 9.5
$|G| < \infty$

1. $\forall a \in G \implies |a| \big| |G|$
2. If $|G| = n \implies a^n = e \quad \forall a \in G$.

Proof.

1. Consider $H = \langle a \rangle \subseteq G$. $|\langle a \rangle| = |a| \implies$ Since $|G| < \infty$
$$\begin{aligned} &\implies H < \infty \text{ we can use Lagrange} \\ &\implies |H| = |\langle a \rangle| = |a| \big| |G|. \end{aligned}$$
2. Suppose $|a| = m$. Then by (1), $m \mid n \implies n = md$ for some $d \in \mathbb{Z}$. So then
$$a^n = a^{md} = (a^m)^d = e^d = e$$

$\square$

9.2 Classification of Groups of Prime Order

Theorem 9.6
Suppose $p > 0$ prime. If $|G| = p \implies G \cong \mathbb{Z}_p$.

Proof. By Theorem 7.10, all cyclic groups of order n are isomorphic to $\mathbb{Z}_n$. $\implies$ We only need to show G is cyclic. Consider $a \in G$ with $a \neq e$. Then $|\langle a \rangle| \neq 1 \implies$ by Lagrange, since $|\langle a \rangle| \mid p$. Since only 1 or p divides $p \implies |\langle a \rangle| = p$. Since $|G| = p$ and $\langle a \rangle \subseteq G$

$$\begin{aligned} \implies G = \langle a \rangle &\implies G \text{ is cylic of order } p \\ &\implies G \cong \mathbb{Z}_p \text{ by previous theorem} \end{aligned}$$

$\square$

9.3 Classification of Groups of Order ≤ 8

We know $\cancel{1}, \underbrace{\cancel{2}, \cancel{3}}_{\text{prime}}, 4, \underbrace{\cancel{5}}, 6, \underbrace{\cancel{7}}, 8$

Theorem 9.7
If $|G| = 4 \implies$ either $G \cong \underbrace{\mathbb{Z}_4}_{\substack{\text{cyclic} \\ \text{abelian}}}$ or $G \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{abelian}}$.

Proof. If $|G| = 4$, then either $\exists a \in G$ with $|a| = 4$ or not.

- If yes, then $G = \langle a \rangle \implies G$ is cyclic $\implies G \cong \mathbb{Z}_4$.
- If not, then $G = \{e, a, b, c\}$, since only e can have order 1, then $|a| = |b| = |c| = 2$

$$\begin{aligned} &\implies a^2 = b^2 = c^2 = e \\ &\implies a = a^{-1}, b = b^{-1}, c = c^{-1} \end{aligned}$$

If $|ab| = 1 \implies a = b^{-1} \implies$ contradiction $|ab| = 2$.

So either

$$\begin{aligned} &ab = a \implies b = e \text{ contradiction} \\ &ab = b \implies a = e \text{ contradiction} \\ &ab = c\checkmark \end{aligned}$$

Repeat this for ac, ca, ba, bc, cb to find entire multiplication table. Then construct an explicit isomorphism to

$$\mathbb{Z}_2 \times \mathbb{Z}_2 : \begin{aligned} e &\mapsto (0, 0) \\ a &\mapsto (1, 0) \\ b &\mapsto (0, 1) \\ c &\mapsto (1, 1) \end{aligned}$$

$\square$

Theorem 9.8
$|G| = 6 \implies G \cong \mathbb{Z}_6$ or S_3.

10 Jan 26, 2022

10.1 Normal Subgroups

Recall 10.1 For $a \in G, H \subseteq G$ subgroup. Right coset $Ha = \{ha \in G \mid h \in H\}$. Left coset $aH = \{ah \in G \mid h \in H\}$.

Definition 10.2 (Normal subgroup)
A subgroup N of G is <u>normal</u> if $Na = aN \; \forall a \in G$.

Note 10.3: $Na = aN \;\not\Longrightarrow\; an = na$. Rather, it means that $an = n'a$ for some $n, n' \in N$.

Notation 10.4: Whenever N is normal in G, we write $N \lhd G$.

Example 10.5
Consider $G = D_4$ (not abelian).
Let $M = \{e, r_{180}\}$ then you can show

$$r_{180} \cdot a = a \cdot r_{180} \quad \forall a \in D_4$$

$$\implies Ma = aM \implies M \lhd D_4$$

Theorem 10.6
If G is abelian, then all subgroups are normal.

Recall 10.7 The center $Z(G) = \{a \in G \mid ag = ga\}$.

Proposition 10.8
For any G, the center $Z(G)$ is always normal.

Proof. Using the definition of $Z(G)$, we notice that for any $g \in G$,

$$Z(G)g = gZ(G)$$

For any $a \in Z(G), ag \in Z(G)g$. Since $ag = ga$ because $a \in Z(G)$ (by definition), then $ga \in gZ(G)$. □

Example 10.9
$S_3 = \{e, \tau_1, \tau_2, \tau_{12}, \tau_{21}, \tau_{121}\}$.
Let $A_3 := \{e, \tau_{12}, \tau_{21}\}$.
Then

$$A_3 a = \left\{ \begin{matrix} \tau_{12} \circ \tau_1 = \tau_{121} = \tau_1 \circ \tau_{21} \\ \tau_{12} \circ \tau_2 = \tau_1 = \tau_2 \circ \tau_{21} \\ \underbrace{\tau_{12} \circ \tau_{121}}_{\in A\tau_{121}} = \tau_2 = \underbrace{\tau_{121} \circ \tau_{21}}_{\in \tau_{121} A} \end{matrix} \right\} = aA_3$$

Recall $(a \in N, aN = N = Na)$

$$\implies A_3 a = aA_3 \quad \forall a \in S_3 \implies A_3 \text{ is normal}$$

Theorem 10.10
For $N \lhd G$, if $Na = Nb$ and $Nd = Nc \implies Nad = Nbc$ (Analogously, $Nda = Ncb$).

Proof. Direct from set definitions of cosets. □

Definition 10.11
Given $a, b \in G, N \subseteq G$,

$$aNb := \{anb \in G \mid n \in N\}$$

Theorem 10.12
TFAE:

1. $N \lhd G$.
2. $a^{-1}Na \subseteq N \quad \forall a \in G$.
3. $aNa^{-1} \subseteq N \quad \forall a \in G$.
4. $a^{-1}Na = N \quad \forall a \in G$.
5. $aNa^{-1} = N \quad \forall a \in G$.

Proof. 1) $\implies$ 3) N normal $\implies aN = Na \implies \forall a \in G$ and $n \in N$

$$\begin{aligned} \exists n' \in N \text{ such that } an = n'a &\implies ana^{-1} = n' \\ &\implies aNa^{-1} \subseteq N \end{aligned}$$

3) $\implies$ 2) Since if $aNa^{-1} \subseteq N$ $\forall a \in G$ and $a^{-1} \in G$

$$(a^{-1})N(a^{-1})^{-1} = a^{-1}Na \subseteq N$$

2) $\implies$ 3) analogous.
4) $\iff$ 5) proved the same way.

3) $\implies$ 4) If $aNa^{-1} \subseteq N$ then since $ana^{-1} \in N \quad \forall a \in G, \forall n \in N$

$$\begin{aligned}
&\overset{\text{by 2)}}{\implies} a^{-1}\underbrace{(ana^{-1})}_{n'}a \in a^{-1}Na \\
&\implies n \in a^{-1}Na \implies N \subseteq \underbrace{a^{-1}Na}_{\iff \text{by 3}} \\
&\implies N \subseteq aNa^{-1} \implies N = aNa^{-1}
\end{aligned}$$

2) $\implies$ 5) same proof as 3) $\implies$ 4).
5) $\implies$ 1)

$$\begin{aligned}
aNa^{-1} = N &\implies ana^{-1} = n' \text{ for some } n' \in N \\
&\implies an = n'a \\
&\implies aN \subseteq Na
\end{aligned}$$

Use the fact 4) $\iff$ 5) to show $Na \subseteq aN$.
$\implies Na = aN \implies N \lhd G$. $\square$

11 Jan 28, 2022

11.1 Quotient Groups

Given $N \lhd G$, let $G/N := \{Na \mid a \in G\}$.

Recall 11.1 If $N \lhd G, Na = Nb$ and $Nc = Nd$, then $\implies Nac = Nbd$.

Theorem 11.2
$N \lhd G$, then

1. G/N is a group with operation $\underbrace{Na \cdot Nb}_{*\text{ operation in } G/N} := \overbrace{Nab}^{\text{product inside } G}$
2. If $|G| < \infty \implies |G/N| = |G|/|N|$
3. If G is abelian $\implies G/N$ is abelian.

We call G/N the quotient group of G by N.

Proof. 1) Check each axiom of groups:

- $id := N$
- Inverse $:= Na^{-1} \implies (Na)(Na^{-1}) = Naa^{-1} = Ne = N$
- etc.

2) $|G/N| = [G{:}N] = |G|/|N|$
3) $\underbrace{(Na)(Nb)}_{Nab} = \underbrace{(Nb)(Na)}_{Nba}$
because G is abelian, $N\underline{ab} = N\underline{ba}$. $\square$

Example 11.3
Consider
$$2\mathbb{Z} = \langle 2 \rangle \subseteq \mathbb{Z}.$$
$\mathbb{Z}$ abelian $\implies 2\mathbb{Z}$ normal.
$$|\mathbb{Z}/2\mathbb{Z}| = [\mathbb{Z}{:}2\mathbb{Z}] = 2$$
$$2\mathbb{Z} = \{-4, -2, 0, 2, 4, \dots\} = \text{ evens}$$
$2\mathbb{Z} + 1 = \text{odds} \implies \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$
Generally,
$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Example 11.4
$A_3 \lhd S_3$
$A_3 = \{e, \tau_{12}, \tau_{21}\}$
$|S_3| = 6, |A_3| = 3$, so

$$|S_3/A_3| = \frac{6}{3} = 2$$
$$\implies S_3/A_3 \cong \mathbb{Z}_2$$

Example 11.5
$N = \langle 4 \rangle = \{0, 4, 8\} \subseteq \mathbb{Z}_{12}$

$$[0] = N + 0 = N$$
$$[1] = N + 1 = \{1, 5, 9\}$$
$$[2] = N + 2 = \{2, 6, 10\}$$
$$[3] = N + 3 = \{3, 7, 11\}$$

$$\implies N + a = N + b \iff a \equiv b \mod 4$$
$$\text{i.e: } N + 6 = \{6, 10, 2\} \quad 6 \equiv 2 \mod 4$$

$\mathbb{Z}_{12}/N \cong$? where $|\mathbb{Z}_{12}/N| = 4$
So either

$$\mathbb{Z}_{12}/N \cong \mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \times \mathbb{Z}_2$$

$[4] = [1] + [1] + [1] + [1] = [0]$
$(N + 1) + (N + 1) + (N + 1) + (N + 1) = N + 4 = N$, because $4 \equiv 0 \mod 4$.
So,

$$|N + 1| = 4 \implies \mathbb{Z}_{12}/N \cong \mathbb{Z}_4$$

Theorem 11.6
$N \lhd G$. Then G/N is abelian if and only if $aba^{-1}b^{-1} \in N \; \forall a, b \in G$.

Proof. G/N is abelian iff $Nab = Nba \; \forall a, b \in G$

$$\iff ab \equiv ba \mod N \; \forall a, b \in G$$
$$\iff aba^{-1}b^{-1} \equiv e \mod N \iff aba^{-1}b^{-1} \in N$$

□

Theorem 11.7
G any group. $G/Z(G)$ is cyclic $\implies$ G abelian.

Proof. If $G/Z(G)$ is cyclic, then $G/Z = \langle Zg \rangle$ for some $g \in G \implies$ every other coset $Zg' = (Zg)^k = Zg^k$. So then if $a, b \in G$, then

$a \in Za = Zg^k$ for some k,
$b \in Zb = Zg^j$ for some j.

$$\begin{aligned} &\implies a = c \cdot g^k \text{ and } b = c'g^j \text{ for some } c, c' \in Z \\ &\implies ab = cg^k \cdot c'g^j = c'g^j cg^k = ba \\ &\implies G \text{ is abelian.} \end{aligned}$$

□

11.2 Quotient Groups and Homomorphisms

Definition 11.8 (Kernel)
Let $\varphi\colon G \to H$ be a homomorphism. The kernel of φ is the set

$$\ker \varphi := \{g \in G \mid \varphi(g) = e_H\}$$

Example 11.9
Consider

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \mathbb{Z}_5 \\ n &\mapsto [n] \end{aligned}$$

Then,

$$\begin{aligned} \ker \varphi &= \{n \in \mathbb{Z} \mid [n] = [0]\} = \{n \mid n \equiv 0 \mod 5\} \\ &= 5\mathbb{Z} \end{aligned}$$

Theorem 11.10
Suppose $\varphi\colon G \to H$ is a homomorphism. Then $\ker \varphi \lhd G$ is a normal subgroup of G.

Proof. Subgroup:

- (Identity): Since $\varphi(e) = e \implies e \in \ker \varphi$
- (Closure): If $a, b \in \ker \varphi$,

$$\begin{aligned} \varphi(ab) = \varphi(a) \cdot \varphi(b) &= e \cdot e = e \\ \implies ab &\in \ker \varphi. \end{aligned}$$

- (Inverse): If $a \in \ker \varphi$, then $\varphi(a^{-1}) = (\varphi(a))^{-1} = e^{-1} = e$

  $\implies \ker \varphi$ is a subgroup.

Normal: We will show $g \ker \varphi g^{-1} \subseteq \ker \varphi \; \forall g \in G$.
Let $a \in \ker \varphi$, so $\varphi(a) = e$. Then any $g \in G$:

$$g\varphi(a)g^{-1} = g \cdot e \cdot g^{-1} = e \in \ker \varphi$$

$$\implies g \cdot \ker\varphi g^{-1} \subseteq \ker\varphi$$

$\square$

12 Jan 31, 2022

12.1 Quotient Groups and Homomorphisms (Cont'd)

Example 12.1
Let

$$\begin{aligned} \varphi\colon S_3 &\to \mathbb{Z}_2 \text{ given by} \\ e, \tau_{21}, \tau_{12} &\mapsto 0 \\ \tau_1, \tau_2, \tau_{121} &\mapsto 1 \end{aligned}$$

- Is a homomorphism? Yes. (Check this).
- Kernel of φ? $\ker\varphi = \{e, \tau_{12}, \tau_{21}\} = A_3$
  By theorem A_3 is normal in S_3. $S_3/A_3 \cong \mathbb{Z}_2$

Theorem 12.2
A homomorphism φ is injective if and only if $\ker\varphi = e$.

Proof. Standard. □

Theorem 12.3
If $N \lhd G$, then

$$\begin{aligned} \pi\colon G &\to G/N \\ a &\mapsto Na \end{aligned}$$

is surjective group homomorphism with $\ker\pi = N$.

Proof. <u>π is surjective:</u> To every coset Na $\exists a \in G$ such that $a \mapsto Na$.
<u>π is homomorphic:</u> $\pi(ab) = Nab = (Na)\cdot(Nb) = \pi(a)\cdot\pi(b)$
<u>$e = N$</u> if $\pi(a) = N \implies Na = N \iff a \in N$ So,

$$\ker\varphi = \{a \in G \mid a \in N\} = N$$

□

Lemma 12.4
Suppose $\varphi\colon G \to H$ is a homomorphism with $\ker\varphi = K$. Then $\forall a, b \in G, \varphi(a) = \varphi(b)$ if and only if $Ka = Kb$.

Proof. $\varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b)^{-1} = e \iff \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) = e \iff ab^{-1} \in \ker\varphi = K \iff a \equiv b \mod K \iff Ka = Kb$ □

12.2 The Isomorphism Theorems

Theorem 12.5 (First Isomorphism Theorem)
Let $\varphi\colon G \to H$ be a surjective homomorphism. Then

$$G/\ker\varphi \cong H$$

Proof. Let

$$\begin{aligned}\pi\colon G/\ker\varphi &\to H\\ Ka &\mapsto \varphi(a)\end{aligned}$$

where $K = \ker\varphi$. We need to show π is a well-defined isomorphism

1. Well-defined: Let $Ka = Kb$ for $a \neq b$. Then $ab^{-1} \in K = \ker\varphi \implies \varphi(ab^{-1}) = e \implies \varphi(a) = \varphi(b)$

2. Homomorphism:

$$\begin{aligned}\pi(Ka \cdot Kb) &= \pi(Kab)\\ &= \varphi(ab) = \varphi(a)\cdot\varphi(b)\\ &= \pi(Ka)\cdot\pi(Kb)\end{aligned}$$

3. Surjective: $\pi\colon G/K \to H$. Let $h \in H$, then $\exists g \in G$ such that $\varphi(g) = h$ because φ is surjective. Consider $Kg \in G/\ker\varphi$. Then $\pi(Kg) = \varphi(g) = h$.

4. Injective: Suppose $\pi(Ka) = \pi(Kb)$

$$\begin{aligned}&\implies \varphi(a) = \varphi(b)\\ &\implies ab^{-1} \in \ker\varphi\\ &\implies Ka = Kb \implies \pi \text{ is 1-1}\end{aligned}$$

□

Theorem 12.6 (Second Isomorphism Theorem)
Suppose N and K are subgroups of G, with $N \lhd G$. Then

$$NK := \{nk \mid n \in N, k \in K\}$$

is a subgroup of G containing both N and K.

Proof. Homework. ☺ □

Lemma 12.7
Let $N \lhd G$, and K is any subgroup of G such that $N \subseteq K$. Then $N \lhd K$ and K/N is a subgroup of G/N.

Proof. Since $aN = Na \; \forall a \in G$ so then if $a \in K$, then $aN = Na \; \forall a \in K$
$\implies N \lhd K \implies K/N$ is a subgroup.
Since

$$K/N = \{Na \mid a \in K\}$$

and since $K \subseteq G \implies K/N \subseteq G/N$. $\square$

Theorem 12.8 (Third Isomorphism Theorem)
Let $K \lhd G, N \lhd G, N \subseteq K \subseteq G$. Then,

1. $K/N \lhd G/N$ and
2. $(G/N)/(K/N) \cong G/K$

13 Feb 2, 2022

13.1 The Isomorphism Theorems (Cont'd)

Proof of Third Isomorphism Theorem. Since $K \lhd G$ and $N \lhd G \implies G/N$ and G/K are groups. Consider

$$\begin{aligned}\varphi\colon G/N &\to G/K \\ Ng &\mapsto Kg\end{aligned}$$

Well-defined:
If $Ng = Ng'$ with $g \neq g'$

$$\begin{aligned}\implies g'g^{-1} \in N \subseteq K &\implies Kg = Kg' \\ &\implies \varphi(Ng) = \varphi(Ng')\end{aligned}$$

Homomorphism:

$$\begin{aligned}\varphi(Ng \cdot Ng') &= \varphi(Ngg') = Kgg' \\ &= Kg \cdot Kg' = \varphi(Ng) \cdot \varphi(Ng')\end{aligned}$$

Surjective: Obvious by definition of the map

$$\varphi\colon G/N \to G/K \quad \forall Kg \to \exists Ng \text{ s.t. } \varphi(Ng) = Kg$$

$\implies$ We can apply the First Isomorphism Theorem so that

$$(G/N)/\ker\varphi \cong G/K$$

We show $\ker\varphi = K/N$: Now, $\varphi(Ng) = K = Ke \iff g \in K$. Then,

$$\ker\varphi = \{Ng \mid g \in K\}$$

By Lemma 12.7, $N \lhd K$ so K/N makes sense. Also, $\ker\varphi = K/N$.
Since by previous theorem, since $\ker\varphi \lhd G/N$ then this means that $K/N \lhd G/N$ and

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

□

Corollary 13.1
Suppose $N \lhd G$ and K is any subgroup of G such that $N \subseteq K \subseteq G$. Then $K \lhd G$ if and only if $K/N \lhd G/N$.

Proof. $(\implies) K \lhd G \implies K/N \lhd G/N$ (by Third Isomorphism Theorem).

($\Longleftarrow$) Suppose $K/N \lhd G/N$. For any $Na \in G/N$, we know

$$(Na)^{-1}(Nk)(Na) \in \underbrace{K/N}_{\ni Nk} \lhd \underbrace{G/N}_{\ni Na}$$

Then $\forall a \in G$ and $k \in K$,

$$Na^{-1}ka = (Na^{-1})(Nk)(Na) \in K/N$$

$$\implies Na^{-1}ka \in K/N$$

So this means $\exists t \in K$ such that

$$Na^{-1}ka = Nt$$

$$\implies \forall n \in N \; \exists n' \in N$$

$$na^{-1}ka = n't$$

$$\implies a^{-1}ka = \underbrace{n^{-1}n't}_{\substack{n,n' \in N \subseteq K \\ t \in K}} \in K.$$

<u>Recall:</u> $K \lhd G$ if and only if $aKa^{-1} \subseteq K \; \forall a \in G$.
Equivalently: $aka^{-1} \in K \quad \forall a \in G \quad \forall k \in K$
$\implies K$ is normal. □

Theorem 13.2 (The Correspondence Theorem)
Suppose $T \subseteq G/N$ is a subgroup. Then there exists some subgroup $H \subseteq G$ with $N \subseteq H$ such that

$$T = H/N$$

i.e. There exists a correspondence between

$$N \subseteq H \subseteq G \longleftrightarrow T \subseteq G/N$$

This theorem classifies all subgroups of G/N.

Proof. Given $T \subseteq G/N$ subgroup. Let $H := \{a \in G \mid Na \in T\}$.

- $N \in T$ since T is a subgroup of $G/N \implies e \in H$.
- If Na and $Nb \in T$ then
  $$Nab = Na \cdot Nb \in T$$
  Since T is closed $\implies ab \in H$.
- If $Na \in T$ then $(Na)^{-1} = Na^{-1} \in T \implies a^{-1} \in H \implies H$ is a subgroup of G.

Now, $\forall a \in N, Na = N$ and since $N \in T$

$$\implies a \in H \; \forall a \in N \implies N \subseteq H.$$

Thus, $N \subseteq H \subseteq G$.

Finally, we must show $T = H/N$. (By Lemma 12.7, $N \lhd G \implies N \lhd H$ so H/N makes sense).
Using the fact that $H = \{a \in G \mid Na \in T\}$,

$$H/N = \{Na \mid a \in H\} = \{Na \in T \mid a \in G\} = T$$

$\square$

14 Feb 4, 2022

14.1 Simple Groups

Definition 14.1 (Simple group)
A group is simple if it has no nontrivial proper subgroups, i.e. the only subgroups it has are e and G.

Example 14.2
$\mathbb{Z}_2, \mathbb{Z}_3, \dots, \mathbb{Z}_p$

By Lagrange, $1 \mid p$ and $p \mid p \implies$ only subgroups of $\mathbb{Z}_p$ are e and $\mathbb{Z}_p$
$\implies \mathbb{Z}_p$ is simple if and only if p is prime.

Theorem 14.3
G is a simple abelian group if and only if $G \cong \mathbb{Z}_p$ for p prime.

Proof. ($\impliedby$) done.
($\implies$) Suppose G is a simple abelian group. Then $\forall a \in G$ with $a \neq e$; $G = \langle a \rangle$. Then G is cyclic $\implies G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$ for some $n \in \mathbb{N}$.
If $G \cong \mathbb{Z}$, G cannot be simple since $\mathbb{Z}$ has infinitely many subgroups (i.e. $n\mathbb{Z}$) $\implies G \cong \mathbb{Z}_n$.
If n is not prime, then $n = kd$ for $k, d \in \mathbb{N}$.
$\implies \langle a^d \rangle \subseteq G$ is a proper subgroup of order k which is a contradiction because G is simple $\implies n$ is prime. So $G \cong \mathbb{Z}_p$. $\square$

$$\longrightarrow \text{Midterm is up to here!} \longleftarrow$$

14.2 The Symmetric Group

Definition 14.4 (Symmetric group)
The symmetric group S_n is the group of permutations of $\{1, \dots, n\}$ where group operation corresponds to composition of permutations. It has order $n!$

Permutation $\implies$ assignment of entry to position a_i

$$\begin{pmatrix} 1 & \dots & i & \dots & n \\ \downarrow & & \downarrow & & \downarrow \\ a_1 & & a_i & & a_n \end{pmatrix}$$

So each permutation is just a bijection $\{1 \dots n\} \to \{1 \dots n\}$.

14.3 Cycle Notation

Example 14.5

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \implies \begin{tikzcd} 1 \arrow[r] & 2 \arrow[r] & 3 \arrow[ll, bend right] \end{tikzcd} \implies \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

Example 14.6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \implies \begin{pmatrix} 1 & 3 & 5 & 2 \end{pmatrix}(4) = \begin{pmatrix} 1 & 3 & 5 & 2 \end{pmatrix}$$

Example 14.7

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1 \quad 2 \quad 3 = (1)(2)(3) = e$$

Example 14.8

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 7 & 2 & 4 & 6 & 3 \end{pmatrix}$$

$$\begin{aligned} (1542)(37)(6) &= (1542)(6)(37) \\ &= (6)(37)(1542) = (37)(1542) \\ &= (1542)(37) \end{aligned}$$

Note: $(2154) = (1542) \neq (5142)$

14.4 Multiplying in Cycle Notation

To compose in cycle notation you "trace" each entry from right to left. Always start with the first entry of the right most cycle.

Example 14.9

$(243)(1243) = (1423)$

Example 14.10

$(12)(34) = (34)(12)$

Can't merge this because the cycles are disjoint

Example 14.11
$(12)(23)(34) = (3412) = (4123) = (1234)$
Check this:

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

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

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

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

$$= (1234)$$

15 Feb 7, 2022

15.1 The Symmetric Group (Cont'd)

Definition 15.1 (Disjoint cycle)
We say two cycles are disjoint if they have no entries in common.

Example 15.2
(12)(358) are disjoint
(132)(358) not disjoint

Theorem 15.3
Disjoint cycles commute.

Proof. Easy and straightforward. □

Theorem 15.4
Every permutation in S_n is a product of disjoint cycles.

Example 15.5
From above (1542)(37)(6) product of disjoint cycles.

Recall 15.6 Order of $g \in G$ is the smallest positive integer k s.t. $g^k = e$.

Theorem 15.7
The order of any $w \in S_n$ is the least common multiple of the lengths of the disjoint cycles of w.

Example 15.8
$w = (1542)(37)$ So,

$$|w| = \text{lcm}(4, 2) = 4$$

Check this by computing $w \neq e$, $\underbrace{w^2, w^3, w^4}_{\text{which of these } = e?}$.

$$\begin{aligned} w^2 &= (1542)(37)(1542)(37) \\ &= (1542)(1542)(37)(37) \end{aligned}$$

And

$$w^4 = \underbrace{(1542)\dots(1542)}_{4\times}\underbrace{(37)(37)(37)(37)}$$

Example 15.9
We have $w = (1243)(243)$. What is $|w|$?
Because (1243)(243) are not disjoint, we need to make them disjoint. By multiplying,

$$(2341) \implies w = (2341) \implies |w| = 4$$

Definition 15.10 (Transposition)
A cycle of length 2 is called a transposition, i.e. (ab) for any $a, b \in \{1 \ldots n\}$.

Definition 15.11 (Simple transposition)
A transposition is simple when $b = a \pm 1$, i.e. $(a\ a+1)$ or $(a-1\ a)$. Or

$$(12), (23), (34), \ldots \text{ etc}$$

Fact 15.12: Simple transpositions generate all of S_n.

Example 15.13
$(1 \quad 5) = (12)(23)(34)(45)$

Proposition 15.14
For any $a, b = \{1 \ldots n\}$

1. (Self-inverses) $(ab)(ab) = e$.
2. Suppose $\sigma_1 \ldots \sigma_k$ are all transpositions.
$$[\sigma_1 \ldots \sigma_k]^{-1} = \sigma_k \sigma_{k-1} \ldots \sigma_1$$
3. Every cycle is a product of (not necessarily disjoint) transpositions, i.e.
$$(a_1 \ldots a_k) = (a_1 a_2)(a_2 a_3) \ldots (a_{k-1} a_k)$$

Example 15.15
$S_3 = \{e, \tau_1, \tau_2, \tau_{21}, \tau_{12}, \tau_{121}\}$.

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

$$\begin{aligned} \implies \tau_{21} &= (23)(12) = (132) \\ \tau_{12} &= (12)(23) = (231) = (123) \\ \tau_{21} &= (12)(23)(12) = (12)(132) = (13)(2) = (13) \end{aligned}$$

<u>Multiplication is easy using this notation:</u>

$$\begin{aligned} \tau_{12} \cdot \tau_{21} &= (23)(12) \cdot (12)(23) \\ &= (23)(23) = e \end{aligned}$$

$$\tau_{212} = (23)(12)(23) = \tau_{121}$$

Theorem 15.16
Every permutation $w \in S_n$ is a product of (not necessarily disjoint) transpositions.

Proof. Combine (3) above in proposition with the fact that every permutation $w \in S_n$ is a product of cycles. □

Corollary 15.17
S_n is generated by simple transpositions, i.e.

$$S_n = \langle (12), (23), (34), \ldots, (n-2, n-1), (n-1, n) \rangle$$

Note there are $n - 1$ generators.

Definition 15.18 (Odd vs. even)
A permutation $w \in S_n$ is:

- <u>Odd</u> if $w =$ product of an odd number of transpositions.
- <u>Even</u> if $w =$ product of an even number of transpositions.

This is known as the <u>parity</u> of a permutation.

Example 15.19
$w = (1542)(37) = (15)(54)(42)(37)$.
Since w is a product of 4 transpositions and 4 is even $\implies$ w is even.

Example 15.20
$w = (2341) = (23)(34)(41)$
$\implies w$ is odd
Notice $|w| = 4$ and w is a product of 3 transpositions. So the order $\neq$ parity. Notice we could have written

$$w = (2341) = (12)(24)(43)(24)(43)$$

$\implies w$ is now a product of 5 transpositions.

16 Feb 9, 2022

16.1 The Symmetric Group (Cont'd)

The parity of a permutation is independent of the choice of decomposition into transpositions.

Lemma 16.1
The identity $e \in S_n$ is even not odd.

Proof. Tedious. Please read in book. □

Theorem 16.2
Every permutation is either even or odd, not both.

Proof. Suppose not. Then $\exists w \in S_n$ such that

$$w = \sigma_1 \dots \sigma_n \quad w = \tau_1 \dots \tau_m$$

where n is even and m is odd

$$\begin{aligned} e = w \dots w^{-1} &= \sigma_1 \dots \sigma_n (\tau_1 \dots \tau_m)^{-1} \\ &= \sigma_1 \dots \sigma_n \tau_m \dots \tau_1 \end{aligned}$$

$\implies$ e is a product of $n + m$ transpositions.
$\implies$ e is odd because $n + m$ is odd.
Which is a contradiction. Thus w is either even or odd, not both. □

16.2 The Alternating Group

Definition 16.3 (Alternating group)
For any given S_n, define the alternating group A_n as the set of all even permutations in S_n.

Theorem 16.4
A_n is a subgroup of S_n of order $\dfrac{n!}{2}$.

Proof. Products and inverses of even permutations remain even. Because $e \in A_n$ by Lemma 16.1. □

Note 16.5: A_n is almost always the only normal simple subgroup of S_n! This fact is crucial to trying to solve quintic and higher order polynomial equations.

Theorem 16.6
$\forall n \neq 4$, A_n is simple.

Proof (Sketch). Idea: decompose permutations in A_n into case by case analysis of the cycle lengths of each one. Basically follows from the next two lemmas. □

Lemma 16.7
For $n \geq 3$, every nonidentity element of A_n is a product of cycles of length 3.

Proof. Consider any pair of transpositions $(ab)(cd)$.

- If $a = c, b = d$: $(ab)(ab) = e$.
- If $a = c$: $(ab)(ad) = (adb)$
- Else: $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$

Since any $w \in A_n$ is a product of an even number of transpositions. $\implies$ This allows you to then write $w =$ product of cycles of length 3. □

Lemma 16.8
If $N \lhd A_n$ and N contains a 3-cycle $\implies N = A_n$. So A_n is simple.

Corollary 16.9
For $n \geq 5$, A_n is the only proper nontrivial normal subgroup of S_n.

Proof. If $N \lhd S_n$ then one can show $N \cap A_n \lhd A_n$. Since A_n is simple either:

- $N \cap A_n = A_n \implies N = A_n$ or $N = S_n$
- $N \cap A_n = e \implies N = e \cup \{w \in S_n \mid w \text{ odd}\}$.

But N is a subgroup and if w, w' are odd, then $w \cdot w'$ is even.
$\implies N$ is not closed if N contains odd permutations and $N = e \cup \{w \in S_n \mid w \text{ odd}\}$.
$\implies N = e$. □

Theorem 16.10 (Cayley's Theorem)
Every group G (finite) is isomorphic to a group of permutations.

Proof. Consider G as a set, let $S(G)$ denote the group of all permutations of the set G. Then,

$$S(G) = \{\text{bijections from } G \to G \text{ under composition}\}$$

Define:

$$\begin{aligned} \varphi\colon G &\to S(G) \\ a &\mapsto \varphi(a) \end{aligned}$$

where

$$\begin{aligned} \varphi(a)\colon G &\to G \\ g &\mapsto ag \end{aligned}$$

The map $\varphi(a)$ is a bijection:

$$\begin{aligned} g_1, g_2 \in G \implies \varphi(a)(g_1) &= \varphi(a)(g_2) \\ ag_1 &= ag_2 \\ g_1 &= g_2 \implies \varphi(a) \text{ is 1-1.} \end{aligned}$$

Given $g \in G$,

$$\varphi(a)(a^{-1}g) = a \cdot (a^{-1}g) = g$$

$\implies \varphi(a)$ is onto.
$\implies \varphi(a)\colon G \to G$ is a bijection $\forall a \in G$.
$\implies \varphi\colon G \to S(G)$ is well-defined.
φ is a homomorphism: Let $a, b, g \in G$.
Want: $\varphi(ab) = \varphi(a) \circ \varphi(b)$

$$\begin{aligned} \varphi(ab)(g) &= \big(\varphi(a) \circ \varphi(b)\big)(g) \quad \forall g \in G \\ abg &= \underbrace{\varphi(a)(bg)}_{abg} \end{aligned}$$

φ is injective: $\forall g \in G$,

$$\begin{aligned} \varphi(a) = \varphi(b) &\implies \varphi(a)(g) = \varphi(b)(g) \\ &\implies ag = bg \\ &\implies a = b \end{aligned}$$

$\implies \varphi$ is injective.
$\implies \varphi\colon G \to S(G)$ is an injective group homomorphism such that $G \cong \operatorname{Im}\varphi \subseteq S(G)$.
$\implies G$ is isomorphic to a group of permutations. $\square$

Corollary 16.11
If $|G| < \infty$ then G is isomorphic to a subgroup of S_n with $n = |G|$.

17 Feb 11, 2022

17.1 Direct Products

Definition 17.1 (Direct product)
Given $G_1, \dots, G_k$ groups, the direct product $G_1 \times \cdots \times G_k$ is the group with elements $(g_1, \dots, g_k)$ with $g_i \in G_i\ \forall i$ and with binary operation:

$$(g_1, \dots, g_k)(g_1', \dots, g_k') = (g_1 g_1', \dots, g_k g_k')$$

Notation 17.2: In additive notation, we denote it instead as direct sum and write it as $G_1 \oplus \cdots \oplus G_k$.

Fact 17.3: $|G_1 \times \dots G_k| = \prod_{i=1}^{k} |G_i|$

Example 17.4
$\mathcal{U}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(1,0,0),(1,1,0),(1,0,1),(1,1,1),(2,0,0),(2,1,0),(2,0,1),(2,1,1)\}$
So,

$$|\mathcal{U}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2| = 2 \times 2 \times 2 = 8$$

Example 17.5
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$.
In this case either notation is fine.

Theorem 17.6
Given $N_i \lhd G$ for $i = 1, \dots, k$. Suppose each $g \in G$ can be uniquely written as a product $g = n_1 \dots n_k$ with $n_i \in N_i\ \forall i$. Then $G \cong N_1 \times N_2 \cdots \times N_k$.

To prove this theorem, we need a lemma:

Lemma 17.7
Suppose $M, N \lhd G$ such that $M \cap N = \{e\}$. If $a \in M$ and $b \in N$ then $ab = ba$.

Proof. Let $a \in M, b \in N$. We need to show that $aba^{-1}b^{-1} \in M \cap N$.

1. Since $M \lhd G$ then $ba^{-1}b^{-1} \in M \implies \underbrace{a}_{\in M} \cdot \underbrace{ba^{-1}b^{-1}}_{\in M} \in M$ because M is closed.

2. Since, $N \lhd G$ then $aba^{-1} \in N \implies \underbrace{aba^{-1}}_{\in N} \cdot \underbrace{b^{-1}}_{\in N} \in N$

3. $aba^{-1}b^{-1} \in M \cap N = \{e\} \implies aba^{-1}b^{-1} = e \implies ab = ba$

□

Proof of Theorem 17.6. Define a map

$$\varphi \colon N_1 \times \dots N_k \to G$$
$$(n_1, \dots, n_k) \mapsto n_1 \dots n_k = g$$

- φ is surjective: follows from the fact that $\forall g$ can be written as $n_1 \dots n_k$.
- φ is injective: follows from the product $n_1 \dots n_k = g$ being unique.
- φ is a homomorphism:
  $(n_1, \dots, n_k), (n_1', \dots, n_k') \in N_1 \times \dots N_k$
  So

$$\begin{aligned}
\varphi\Big((n_1, \dots, n_k) \cdot (n_1', \dots, n_k')\Big) &= \varphi\Big((n_1 n_1', \dots, n_k n_k')\Big) \\
&= n_1 n_1' \cdot n_2 n_2' \cdot \dots n_{k-1} n_{k-1}' \cdot n_k n_k' \\
&= n_1 n_1' \cdot n_2 n_2' \cdot \dots n_{k-2}' n_{k-1} n_k n_{k-1}' n_k' \\
&= n_1 n_1' \cdot n_2 n_2' \cdot \dots n_{k-1} n_{k-2}' n_k n_{k-1}' n_k' \\
&= n_1 n_1' \cdot n_2 n_2' \cdot \dots n_{k-1} n_k n_{k-2}' n_{k-1}' n_k' \\
&\;\;\vdots \\
&= n_1 n_2 \dots n_k \cdot n_1' \dots n_{k-1}' n_k' \\
&= \varphi(n_1, \dots, n_k) \cdot \varphi(n_1', \dots, n_k')
\end{aligned}$$

$\implies \varphi$ is an isomorphism $\implies G \cong N_1 \times \dots \times N_k$. □

Definition 17.8 (Direct product and direct factor)
Whenever $G = N_1 \times \dots \times N_k$ we say G is the <u>direct product</u> of the $N_1's$ and each N_1 is a <u>direct factor</u>.

Definition 17.9
Given $N, M \subseteq G$, subgroups, let $MN = \{mn \in G \mid m \in M, n \in N\}$. Note MN is not necessarily a group.

Theorem 17.10
If $M, N \lhd G$ such that $G = MN$ and $M \cap N = \{e\}$. Then $G = M \times N$.

Proof. By Theorem 17.6 we only need to show uniqueness.
Suppose $g \in G$ such that $g = mn$ and $g = m'n'$ and $m, m' \in M, n, n' \in N$.
$\implies mn = m'n' \implies \underbrace{(m')^{-1} \cdot m}_{\in M} = \underbrace{n'n^{-1}}_{\in N}$
$\implies (m')^{-1}m$ and $n'n^{-1} \in M \cap N = \{e\}$
$\implies n'n^{-1} = e \implies n' = n$ and $(m')^{-1}m = e \implies m' = m$
$\implies g = mn$ is a unique decomposition. □

18 Feb 14, 2022

18.1 Midterm

19 Feb 16, 2022

19.1 Direct Products (Cont'd)

Recall 19.1 If $M, N \lhd G, G = MN, M \cap N = \{e\} \implies G = M \times N$.

Example 19.2
Consider $\underbrace{\mathcal{U}_{15}}_{G} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$$N = \{1, 2, 4, 8\} \quad M = \{1, 11\}$$

- N, M are normal subgroups of $\mathcal{U}_{15}$.
- $M \cap N = \{e\}$
- $\mathcal{U}_{15} = MN$
  We want to show that 7, 13, 14 are products mn for some $m \in M, n \in N$.

$$\begin{aligned} 7 &\equiv 11 \cdot 2 \mod 15 \\ 13 &\equiv 11 \cdot 8 \mod 15 \\ 14 &\equiv 11 \cdot 4 \mod 15 \end{aligned}$$

$\implies \mathcal{U}_{15} = MN$. By theorem, $U_{15} \cong M \times N$.

$$\underbrace{N = \{1, 2, 4, 8\}}_{|N|=4} \quad \underbrace{M = \{1, 11\}}_{|M|=2 \implies M = \mathbb{Z}_2}$$

Check whether N has an element of order 4.
$|1| = 1, |2| = 4$ We know

$$2 \cdot 2 \cdot 2 \cdot 2 = 16 \equiv 1 \mod 15$$

$$2^4 \equiv 1 \mod 15$$

$$\implies \mathcal{U}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

19.2 Finite Abelian Groups

Step 1: Change to additive notation.

$$\begin{aligned} ab &\longmapsto a + b \\ a^k &\longmapsto k \cdot a \\ e &\longmapsto 0 \\ MN &\longmapsto M + N = \{m + n \mid m \in M, n \in N\} \\ M \times N &\longmapsto M \oplus N \\ \text{direct factors } &\longmapsto \text{ direct summands} \end{aligned}$$

Definition 19.3
G-abelian group, p-prime.

$$G(p) := \{a \in G \mid \underbrace{|a| = p^n}_{p^n \cdot a = 0} \text{ some } n \geq 0\}$$

Proposition 19.4
$G(p)$ is a subgroup of G.

We will show: $G = \bigoplus_{p_i} G(p_i)$

Lemma 19.5
G-abelian group, $a \in G$ with $|a| = p_1^{n_1} \dots p_k^{n_k} < \infty$ with p_i prime, $p_i \neq p_j, i \neq j$. Then, $a = a_1 + \dots + a_k$ with $a_i \in G(p_i)$ each i.

Proof. Proof by induction on k.
Base case: $(k = 1)$ $|a| = p_1^{n_1}$.
By definition of $G(p_1) \implies a \in G(p_1)$.
Inductive step: Suppose statement is true for elements that are divisible by at most $k-1$ distinct primes. Then if $|a| = p_1^{n_1} \dots p_k^{n_k}$, let $m = p_1^{n_1} \cdots p_{k-1}^{n_{k-1}}$

$$\implies (m, p_k^{n_k}) = 1$$

$$\implies \exists u_1 v \text{ such that } 1 = um + vp_k^{n_k}$$

Rewrite

$$a = 1 \cdot a = \underbrace{(um)a}_{\in G(p_k)} + (vp_k^{n_k})a$$

$$\implies p_k^{n_k}(uma) = u \cdot (p_k^{n_k} ma) = 0$$

because

$$|a| = p_1^{n_1} \cdots p_k^{n_k} = mp_k^{n_k} \implies (p_k^{n_k} \cdot ma) = 0 \implies uma \in G(p_k).$$

Likewise:

$$m(vp_k^{n_k} a) = v(mp_k^{n_k} a) = 0 \implies vp_k^{n_k} a \text{ has order } m.$$

Since m is a product of $k-1$ primes $\implies$ induction hypothesis applied to $vp_k^{n_k} a$

$$\implies vp_k^{n_k} a = a_1 + \dots + a_{k-1} \text{ with } a_i \in G(p_i) \quad 1 \leq i \leq k-1$$

$$a = 1 \cdot a = \underbrace{(um)a}_{\in G(p_k)} + \underbrace{(vp_k^{n_k})a}_{\implies a_1 + \dots + a_{k-1}}$$

$$\implies a = \underbrace{a_1}_{G(p_1)} + \dots + \underbrace{a_{k-1}}_{G(p_{k-1})} + \underbrace{a_k}_{G(p_k)}$$

□

Theorem 19.6
G-abelian group with $|G| = p_1^{n_1} \cdots p_k^{n_k} < \infty$, p_i are distinct primes. Then

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

Proof. If $a \in G, |a| \Big| |G|$, so we can write

$$a = a_1 + \cdots + a_k \text{ with } a_i \in G(p_i) \text{ each } i$$

where some a_i may be zero. This tells us that there exists such a decomposition. We need to prove uniqueness.
Suppose it's not unique.

$$a = a_1 + \cdots + a_k = b_1 + \cdots + b_k$$

where $a_i, b_i \in G(p_i)$ each i.

$$\implies (a_1 - b_1) + (a_2 - b_2) + \cdots + (a_k - b_k) = 0$$

$$\implies \underbrace{(a_1 - b_1)}_{\in G(p_1)} = \underbrace{(b_2 - a_2)}_{\in G(p_2)} + \cdots + \underbrace{(b_k - a_k)}_{\in G(p_k)}$$

$$\implies p_2^{n_1} \cdots p_k^{n_k}(a_1 - b_1) = 0 \text{ for some } n_i \in N$$

$$\implies \underbrace{|a_1 - b_1|}_{\in G(p_1)} \Big| p_2^{n_2} \ldots p_k^{n_k}$$

$$\implies p_1^{n_1} \Big| p_2^{n_2} \ldots p_k^{n_k}$$

which is impossible for $p_1^{n_1} \geq p_1 \implies n_1 = 0$

$$\implies |a_1 - b_1| = p_1^{n_1} = p_1^0 = 1$$

$a_1 - b_1 = 0 \implies a_1 = b_1 \implies$ by doing the same thing for each

$$(a_1 - b_1) \implies a_1 = b_1 \quad \forall i$$

This proves uniqueness.

$$\implies G = G(p_1) \oplus \cdots \oplus G(p_k)$$

$\square$

20 Feb 18, 2022

20.1 Finite Abelian Groups (Cont'd)

Recall 20.1 G-abelian with $|G| = p_1^{n_1} \dots p_k^{n_k} < \infty$

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

Definition 20.2 (p-group)
For p-prime, a p-group is a group G such that $G = G(p)$.

Fact 20.3: If G-p group, $a \in G$ has maximal order with $|a| = p^n$ then $\forall b \in G, b \neq a$

- $|b| = p^j$ with $j \leq n$
- $p^n \cdot b = 0$ (additive notation)

If $|G| < \infty$ then maximal order elements always exist.

Example 20.4
- $G = \mathbb{Z}_{p^k} \implies |G| = p^k$
- $G = \mathbb{Z}_2 \times Z_2$
- $G = D_4, \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Lemma 20.5
G-finite abelian p-group and $a \in G$ with maximal order. Then there exists a subgroup $K \subseteq G$ such that $G = \langle a \rangle \oplus K$.

Proof. Let K be the largest subgroup of G such that $K \cap \langle a \rangle = 0$. ($G$ finite $\implies$ K exists). G abelian $\implies$ $K \lhd G$ and $\langle a \rangle \lhd G$.
By Theorem 17.1, since $K \lhd G, \langle a \rangle \lhd G$ and $K \cap \langle a \rangle = 0$, to show that $G = K \oplus \langle a \rangle$ we need only show that $G = K + \langle a \rangle$.
Suppose that $G \neq K + \langle a \rangle \implies \exists b \in G$ s.t $b \notin K + \langle a \rangle$.
In particular $b \neq a$ where a is the max order element. Then since G is a p-group and b is not a max element then

$$p^j b = 0 \text{ for some } j \quad (|b| = p^j).$$

Let $r =$ smallest possible integer such that

$$\left.\begin{matrix} p^r b \in \langle a \rangle + K \\ 0 \in \langle a \rangle + K, r \leq j \end{matrix}\right\} \implies p^r b = ta + k \quad (t \in \mathbb{Z}, k \in K)$$

Suppose $|a| = p^n$ so that $p^n a = 0$ then

$$p^n b = 0 \quad \forall b \in G \text{ since } a \text{ is maximal}$$

So,

$$\begin{aligned}p^n(p^{r-1}b) &= p^{n-1}(p^r b)\\ &= p^{n-1}(ta+k) = 0\end{aligned}$$

Therefore,

$$\begin{aligned}&\implies p^{n-1}ta + p^{n-1}k = 0\\ &\implies \underbrace{p^{n-1}ta}_{\langle a\rangle} = \underbrace{-p^{n-1}k}_{\in K} \in \langle a\rangle \cap K = 0\\ &\implies p^{n-1}ta = 0 \text{ and } -p^{n-1}k = 0\\ &\implies |a| = p^n \implies p^n \mid p^{n-1}t\\ &\implies p \mid t \implies t = pm \text{ for some } m\end{aligned}$$

So

$$\left.\begin{aligned}p^r b &= ta + k\\ p^r b &= pma + k\end{aligned}\right\} \implies \begin{cases}k = p^r b - pma\\ \quad = p(p^{r-1}b - ma) \in K\end{cases}$$

If $p^{r-1}b - ma \in K$

$$\begin{aligned}&\implies p^{r-1}b - ma = k' \text{ with } k' \in K\\ &\implies p^{r-1}b = \underbrace{k'}_{\in K} + \underbrace{ma}_{\in\langle a\rangle} \in K + \langle a\rangle\end{aligned}$$

But $r-1 < r$ and we said that r was the smallest integer such that $p^r b \in K + \langle a\rangle$, a contradiction

$$\implies p^{r-1} - ma \notin K.$$

Let $H \coloneqq \{x + z(p^{r-1}b - ma) \mid x \in K, z \in \mathbb{Z}\}$. Then

1. H is a subgroup of G
2. $K \subseteq H$ (take $z = 0$)
3. $K \neq H$ because $z = 1, x = 0$ then $p^{r-1}b - ma \in H$ not in K

Since K is the largest subgroup of G such that $K \cap \langle a\rangle = 0$

$$\implies H \cap \langle a\rangle \neq 0$$

$$\implies \exists w \in H \cap \langle a\rangle \text{ s.t. } w \neq 0$$

Note that $K \cap \langle a\rangle = 0 \implies w \notin K$

$$\implies w = sa = x + z(p^{r-1}b - ma) \text{ for some } s, z \in \mathbb{Z}, x \in K.$$

If $p \mid z$ then $z = qp \implies z(p^{r-1}b - ma) \in K$ since $p(p^{r-1}b - ma) \in K$

$$\implies w = \underbrace{x}_{\in K} + \underbrace{z(p^{r-1}b - ma)}_{\in K} \in K$$

A contradiction, so $p \nmid z \implies (p,z) = 1$ this means $1 = up + vz$ for some $u, v \in \mathbb{Z}$ So

$$\begin{aligned} p^{r-1}b &= (up+vz)p^{r-1}b \\ &= up^r b + vzp^{r-1}b \\ &= u(pma+k) + v(sa - x + zma) \\ &= \underbrace{\underbrace{(upm + vs + zm)}_{\text{numbers}} a}_{\text{multiple of } a \in \langle a \rangle} + \underbrace{(uk - vx)}_{\in K} \\ &\implies p^{r-1}b \in K + \langle a \rangle \end{aligned}$$

a contradiction because r was the smallest integer such that $p^r b \in K + \langle a \rangle \implies b$ cannot exist. So we're done and

$$G = K + \langle a \rangle$$

By previous theorem, since $\langle a \rangle, K \lhd G$ and $\langle a \rangle \cap K = 0$ and $G = K + \langle a \rangle \implies \langle a \rangle \oplus K = G$. $\square$

Theorem 20.6 (The Fundamental Theorem of Finite Abelian Groups (I) (Existence))
Every finite abelian group G is the direct sum of cyclic p-groups i.e. there exists such a decomposition for G s.t.

$$G \cong \bigoplus_i \mathbb{Z}_{p_i^{r_i}} \text{ over some primes (possibly repeated)}$$

21 Feb 23, 2022

21.1 Finite Abelian Groups (Cont'd)

Proof of The Fundamental Theorem of Finite Abelian Groups (I). By Theorem 19.6:

$$G \cong \underbrace{G(p_1)}_{p\text{-groups}} \oplus \cdots \oplus \underbrace{G(p_k)}_{p\text{-groups}}$$

with $|G| = p_1^{n_1} \cdots p_k^{n_k}$. So we only need to show that each p-group $G(p_i)$ = direct sum of cyclic groups.

Proof is by induction on $|G(p_i)| = n$.

Base case: $n = 2$. Then by previous theorem $|G(p_i)| = 2 \implies G(p_i) = \mathbb{Z}_2$.

Inductive Step: Suppose the result holds for any finite abelian group of order $< n$. Let $a \in G(p_i)$ with maximal order. Let $|a| = p_i^m$ for some $m > 0$.

Since $G(p_i)$ is a finite abelian p-group, so by Lemma 20.5 $\implies G(p_i) = \langle a \rangle + K$ for some $K \subseteq G(p_i)$.

Note: $|K| < |G(p_i)| = n$. By induction hypothesis: K = direct sum of cyclic groups.

$$\langle a \rangle = \mathbb{Z}_{p_i^m} \text{ and } K = \bigoplus_i \mathbb{Z}_{p_i^{s_i}}$$

$$\implies G(p_1) = \langle a \rangle \oplus K = \bigoplus_i \mathbb{Z}_{p_i^{s_i}} \oplus \mathbb{Z}_{p_i^m}$$

for possibly repeated primes. □

Example 21.1

Suppose G is a finite abelian group.

1. $|G| = 42 = 7 \cdot 3 \cdot 2$

   $\implies G \cong \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$

2. $|G| = 72 = 3^2 \cdot 2^3$

   - $\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^3}$
   - $\mathbb{Z}_{3^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2}$
   - $\mathbb{Z}_{3^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
   - $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$
   - $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2}$
   - $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

   Note that these are all different and G could be any of these!

Question 21.2: Why does $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$ not show up?

$6 \neq p^n$ but $6 = 3 \cdot 2$ different primes. So, $\mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$

$$\begin{aligned}\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 &= \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ &= \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ &= (\mathbb{Z}_3)^2 \oplus (\mathbb{Z}_2)^3\end{aligned}$$

Lemma 21.3
If $(m,k) = 1$. Then $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.

Proof. $\mathbb{Z}_{mk} = \langle 1 \rangle$ where 1 has order mk. By previous theorem, if G is cyclic of order $n \implies G \cong \mathbb{Z}_n \implies$ suffices to show $\mathbb{Z}_m \oplus \mathbb{Z}_k$ is cyclic of order mk.

1. $\mathbb{Z}_m \oplus \mathbb{Z}_k = \langle (1,1) \rangle$ since by Chinese Remainder Theorem,

$$\begin{aligned}(m,k) = 1 &\implies \exists r \text{ s.t. } r \equiv a \mod m \\ &\qquad\qquad\quad r \equiv b \mod k \\ &\implies (a,b) = r(1,1)\end{aligned}$$

   $\implies$ any $(a,b) \in \mathbb{Z}_m \oplus \mathbb{Z}_k$ can be expressed
   $r(1,1) \implies \langle (1,1) \rangle = \mathbb{Z}_m \oplus \mathbb{Z}_k$.

2. If $t(1,1) = 0, t \equiv 0 \mod m, t \equiv 0 \mod k$

   But $(m,k) = 1 \implies t = \operatorname{lcm}(m,k) = mk \implies |(1,1)| = mk \implies \mathbb{Z}_m \oplus \mathbb{Z}_k$ has order mk, is cyclic $\implies \mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.

□

Example 21.4
- $\mathbb{Z}_6 \oplus \mathbb{Z}_4 \ncong \mathbb{Z}_{24}$ because $(6,4) \neq 1$.

  Note $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \ncong \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$

- $\mathbb{Z}_9 \ncong \mathbb{Z}_3 \oplus \mathbb{Z}_3$ because $(3,3) \neq 1$.

Theorem 21.5
Suppose $n = p_1^{n_1} \cdots p_k^{n_k}$ with p_i are distinct primes. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$.

Proof. Induction on number of factors k. □

22 Feb 25, 2022

22.1 Finite Abelian Groups (Cont'd)

Corollary 22.1
If G is any finite abelian group then G is the direct sum of cyclic groups of orders $m_1, \dots, m_t$ such that $m_i \mid m_{i+1}$ for all i.

Idea of proof. $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_5$.
$\implies G = \mathbb{Z}_2 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{8820}$
So, $2 \mid 30$ and $30 \mid 8820$. $\square$

Corollary 22.2
Suppose $\mathbb{F}$ is a field. If G is a finite subgroup of $\mathbb{F}^*$, then G is cyclic.

Proof. Exercise. $\square$

Definition 22.3 (Invariant factors and elementary divisors)
The numbers m_i in Corollary 22.1 are the invariant factors of G. The prime powers $p_i^{n_i}$ arise in the fundamental theorem of finite abelian groups are the elementary divisors. Suppose

$$G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

then $m_i \mid m_{m+1}$ are the invariant factors and

$$G = \bigoplus_i \mathbb{Z}_{p_i^{n_i}}$$

are the elementary divisors which are potentially repeated primes.

Fact 22.4: The elementary divisors (and the invariant factors) uniquely determine the group (finite abelian) up to isomorphism.

Theorem 22.5 (Fundamental Theorem of Finite Abelian Groups II (Uniqueness))
Suppose G and H are finite abelian groups. Then $G \cong H$ if and only if G and H have the same elementary divisors.

Proof. "$\impliedby$" $G \cong \bigoplus \mathbb{Z}_{p_i^{n_i}}$ and $H \cong \bigoplus \mathbb{Z}_{p_i^{n_i}} \implies$ obviously $G \cong H$.
"$\implies$" Suppose $\varphi\colon G \to H$ is an isomorphism $\implies \forall a \in G$ then $|a| = |\varphi(a)| \implies \forall$ primes $p \big| |G|$ we must have $\varphi(G(p)) = H(p)$.
Thus, we can assume that G and H have the same p-groups. So we only need to prove that p-groups have the same elementary divisors.
Suppose $G = G(p)$ and $|G| = n$. Induct on n.
Base case: $n = 2, G \cong \mathbb{Z}_2 \implies H \cong \mathbb{Z}_2$.
Inductive step: Suppose it's true for all groups of orders less than n.

Since G and H are p-groups, then:

$$G = \mathbb{Z}_p^{n_1} \oplus \mathbb{Z}_{p^2}^{n_2} \oplus \cdots \oplus \mathbb{Z}_{p^t}^{n_t} \quad n_i \in \mathbb{Z}_{\geq 0}$$

$$H = \mathbb{Z}_p^{m_1} \oplus \mathbb{Z}_{p^2}^{m_2} \oplus \cdots \oplus \mathbb{Z}_{p^k}^{m_k} \quad m_i \in \mathbb{Z}_{\geq 0}$$

Consider $pG = \{pg \mid g \in G\}$.
$pG \subseteq G$ subgroup of G with direct summands $p\mathbb{Z}_{p^i} = \langle pa \rangle$ where $\mathbb{Z}_{p^i} = \langle a \rangle$. Exercise
Then $|pa| = p^{i-1}$ since $|a| = p^i \implies p\mathbb{Z}_{p^i}$ is cyclic of order p^{i-1}

$$\implies p\mathbb{Z}_{p^i} = \mathbb{Z}_{p^{i-1}} \implies pG \cong \mathbb{Z}_p^{n_2} \oplus \cdots \oplus \mathbb{Z}_{p^{i-1}}^{n_t}$$

$$\implies pH \cong \mathbb{Z}_p^{m_2} \oplus \cdots \oplus \mathbb{Z}_{p^{k-1}}^{m_k}$$

<ins>Exercise:</ins> $\varphi(pG) = pH \implies pH \cong pG$
By the induction hypothesis since $|pH| < |H|$ and $|pG| < |G| \implies$ the elementary divisors of pH and pG are the same.

$$\implies t = k \text{ and } n_i = m_i \quad \forall i \geq 2$$

All we need now is to show that $n_1 = m_1$.
Recall $G \cong H \implies |G| = |H|$

$$\implies p_1^{n_1} p_2^{n_2} \dots p_t^{n_t} = p_1^{m_1} p_2^{n_2} \dots p_t^{n_t}$$

$$\implies p^{n_1} = p^{m_1}$$

$$\implies n_1 = m_1$$

□

22.2 Sylow Theorems

Question 22.6: What if the groups aren't abelian? How do you classify those.

This is hard. We are going to start this theory by looking at the Sylow theorems.

Definition 22.7 (Conjugate)
Two elements $a, b \in G$ are <ins>conjugate</ins> if there exists $g \in G$ such that $b = g^{-1}ag$.

Example 22.8
$(13) = \underbrace{(12)}_{g^{-1}}(23)\underbrace{(12)}_{g}$
$\implies$ (13) and (23) are conjugate.
$(13) = (23)(12)(23) \implies$ (13) and (12) are conjugate.

Proposition 22.9
Conjugacy is an equivalence relation in G.

Definition 22.10 (Conjugacy classes)
Equivalence classes $\implies$ conjugacy classes $\implies$

- Conjugacy classes are either disjoint or the same.
- $G = \bigcup$ conjugacy classes.

Definition 22.11 (Centralizer)
The centralizer of $a \in G$ is

$$\begin{aligned} C(a) &:= \{g \in G | g^{-1}ag = a\} \\ &= \{g \in G | ga = ag\} \end{aligned}$$

Note 22.12: This is similar but different to center

$$Z(G) = \{a \in G | ag = ga, \forall g \in G\}$$

Theorem 22.13
$C(a)$ is a subgroup of $G, \forall a \in G$.

Proof. Standard. □

23 Feb 28, 2022

23.1 Sylow Theorems (Cont'd)

By partioning G into conjugacy classes,

Definition 23.1 (Orbit)
$[a] = [b]$ if and only if $b = g^{-1}ag$ for some $g \in G$. We call the elements $b \in [a]$ the orbit of a under conjugation.

Theorem 23.2
Suppose $|G| < \infty, a \in G$. Then

$$|[a]| = [G\colon C(a)] = \frac{|G|}{|C(a)|}$$

Proof. Recall $[G\colon C(a)] =$ the number of right cosets of $C(a)$ in G. Let $C = C(a)$ and

$$S = \{Cg \mid g \in G\} \text{ be right cosets of } C(a).$$

Define:

$$\begin{aligned} \varphi\colon S &\to [a] \\ Cg &\mapsto g^{-1}ag \end{aligned}$$

φ well defined: $Cg_1 = Cg_2 \implies g_1g_2^{-1} \in C$

$$\begin{aligned} &\implies (g_1g_2^{-1})a(g_1g_2)^{-1} = a \\ &\implies (g_1g_2^{-1})a(g_2g_1^{-1}) = a \\ &\implies g_2^{-1}ag_2 = g_1^{-1}ag_1 \\ &\implies \varphi(Cg_2) = \varphi(Cg_1) \end{aligned}$$

φ is injective: Suppose $\varphi(Cg_1) = \varphi(Cg_2)$. If $g_1^{-1}ag_1 = g_2^{-1}ag_2$

$$\begin{aligned} &\implies (g_2g^{-1})a(g_2g_1^{-1})^{-1} = a \\ &\implies Cg_2g_1^{-1} = C \\ &\implies Cg_1 = Cg_2 \end{aligned}$$

$\implies \varphi$ is injective.
φ surjective: If $b \in [a]$, there exists x such that $b = x^{-1}ax$ and so then

$$\varphi(Cx) = x^{-1}ax = b.$$

$\implies \varphi$ is a bijection $S \to [a]$

$$\implies [G\colon C(a)] = |S| = |[a]|$$

$\square$

Corollary 23.3
$|[a]|\Big||G|$

Proof. Lagrange. If $a \in Z(G)$,

$$\implies ag = ga \quad \forall g \in G.$$

$[a] = \{a\}$ since

$$g^{-1}ag = a \quad \forall g \in G$$

$$\implies |[a]| = 1 \quad \forall a \in Z(G).$$

□

Definition 23.4 (The class equation)
Suppose $|G| < \infty$. Let $a_1, \ldots, a_n$ denote representations for the distinct conjugacy classes of G:

1. $|G| = \displaystyle\sum_{i=1}^{n} \Big|[a_i]\Big|$
2. $|G| = \displaystyle\sum_{i=1}^{n} [G\colon C(a_i)]$
3. $|G| = \underbrace{|Z(G)|}_{|[a_i]|=1} + \underbrace{\displaystyle\sum_{a_i \notin Z(G)} \Big|[a_i]\Big|}_{|[a_i]|>1}$

Theorem 23.5 (Cauchy's Theorem for Finite Abelian Groups)
If G is a finite abelian group and p is prime such that $p\Big||G| \implies \exists g \in G$ such that $|g| = p$.

Proof. By Fundamental Theorem of Finite Abelian Groups,

$$G \cong \bigoplus_i \mathbb{Z}_{p_i^{n_i}}$$

where p_i are potentially repeated primes, $n_i \in \mathbb{N}$ and $p_i\Big||G|$.
Then consider $e_i = (0, \ldots, 1, 0 \ldots 0)$ with 1 in position i

$$\implies \langle e_i \rangle \cong \mathbb{Z}_{p_i^{n_i}} \text{ cyclic subgroup of } G$$

$$1 = (e_i)^{p_i^{n_i}} = \left(e_i^{p_i^{n_i-1}}\right)^{p_i} \implies \left|e_i^{p_i^{n_i-1}}\right| = p_i$$

□

23.2 First Sylow Theorem

Theorem 23.6 (First Sylow Theorem)
Suppose $|G| < \infty$, and p is prime with $p^k \Big| |G|$ for some k. Then G has a subgroup of order p^k.

Proof. Induction on $|G|$.
Base case: $|G| = 1 \implies G = e$.
Since
$$p^0 \mid 1 \quad \forall \text{ prime } p$$
and $G \supseteq \langle e \rangle$ where
$$|\langle e \rangle| = p^0 = 1.$$
Inductive Step: Suppose this is true for all groups of orders less than $|G|$.
Let $[a_i]$ denote the conjugacy classes of G.
Lagrange $\implies |G| = [G\colon C(a_i)] \cdot |C(a_i)|$ for all i

1. If $\exists a_j \notin Z(G)$ such that $p \nmid [G\colon C(a_j)]$
$$\implies p \mid [C(a_j)]$$
$$\implies \exists k \text{ s.t. } p^k \mid [C(a_j)]$$
Since $a_j \notin Z(G)$
$$\implies [G\colon C(a_j)] > 1$$
$$\implies |C(a_j)| < |G|$$
Then by the induction hypothesis, this implies there exists a subgroup of order p^k inside $C(a_j)$
$$\implies H \subseteq C(a_j) \subseteq G.$$

We will continue this proof in the next lecture. □

24 Mar 2, 2022

24.1 First Sylow Theorem (Cont'd)

Proof of First Sylow Theorem (Cont'd). 2) If $p\Big||G|$ and $p \mid [G\colon C(a_i)]$ $\forall a_i \notin Z(G)$. Then by class equation:

$$\implies |Z(G)| = \underbrace{|G|}_{\text{divisible by } p} - \underbrace{\sum_{a_i \notin Z(G)} [G\colon C(a_i)]}_{\text{divisible by } p}$$

$$\implies p\Big||Z(G)|$$

Note: $Z(G)$ is a finite abelian group. Cauchy's Thoerem says that since $p\Big||Z(G)|$ then there exists $x \in z(G)$ such that $|x| = p$.
Consider $\langle x \rangle \lhd G$ with $|\langle x \rangle| = p$, then

$$|G/\langle x \rangle| = |G|/p < |G|$$

also $p^{k-1}\Big||G/\langle x \rangle| \implies$ by the induction hypothesis that $G/\langle x \rangle$ contains a subgroup T of order p^{k-1}.
By Correspondence Theorem:

$$\underbrace{T \subseteq G/\langle x \rangle}_{\text{subgroups}} \longleftrightarrow \underbrace{\langle x \rangle \subseteq H \subseteq G}_{\text{subgroups containing } \langle x \rangle}$$

where $T = H/\langle x \rangle$.
Thus,

$$p^{k-1} = |H/\langle x \rangle| = \frac{|H|}{|\langle x \rangle|} = \frac{|H|}{p}$$

$\implies |H| = p^k$. Then $H \subseteq G$ is a subgroup of order p^k. $\square$

Corollary 24.1 (Cauchy's Theorem for finite groups)
Suppose $|G| < \infty$ with $p\Big||G|$, then $\exists g \in G$ such that $|g| = p$.

Proof. Immediate from First Sylow Theorem by taking $k = 1$. $\square$

Definition 24.2 (Sylow-p-subgroup)
If $|G| < \infty$ and p is prime, a subgroup $H \subseteq G$ with $|H| = p^n$ is Sylow-p-subgroup if n is the largest positive integer such that $p^n \mid ||G|$. This subgroup always exists by First Sylow Theorem.

Example 24.3
Consider $|S_8| = 8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7$.
First Sylow Theorem guarantees there exists subgroups of order:

- $2, 2^2, 2^3, 2^4, \ldots, 2^7$
- $3, 3^2$
- 5
- 7

Where

- 2^7 are Sylow 2 subgroups
- 3^2 are Sylow 3 subgroups
- 5 are Sylow 5-subgroups
- 7 are Sylow 7-subgroups

Note 24.4: First Sylow Theorem does not guarantee uniqueness.

Example 24.5
Consider $|S_3| = 3! = 3 \cdot 2$
S_3 contains subgroups of orders

- 2
- 3

Since S_3 is very small, then every nontrivial subgroup is a Sylow-p-subgroup.

Goal: Play a similar conjugation game with sets instead of elements.

Proposition 24.6
Suppose H is a Sylow-p-subgroup of G. Then

$$g^{-1}Hg \coloneqq \{g^{-1}hg \in G \mid h \in H\}$$

is also a Sylow p-subgroup of $G, \forall g \in G$.
So $|g^{-1}Hg| = p^n$.

Proof. Recall

$$\begin{aligned} \varphi_g \colon G &\to G \\ x &\mapsto g^{-1}xg \end{aligned}$$

φ_g is an isomorphism, that takes

$$\varphi_g(H) = g^{-1}Hg \implies H \cong g^{-1}Hg$$

$\square$

25 Mar 4, 2022

25.1 K-conjugacy and Normalizers

Definition 25.1 (K-conjugate, conjugate to)
For a fixed subgroup $K \subseteq G$, we say two subgroups H_1 and H_2 are K-conjugate if there exists $k \in K$ such that

$$H_1 = k^{-1} H_2 k$$

If $K = G$, then we say H_1 is conjugate to H_2.

Theorem 25.2
Given any subgroup $K \subseteq G$, K-conjugacy is an equivalence relation on subgroups of G.

Proof. Exercise. □

Definition 25.3 (Normalizer)
The normalizer of a subgroup $A \subseteq G$ is the set

$$N(A) := \{g \in G \mid g^{-1} A g = A\}$$

Remark 25.4 $N(A)$ is basically the centralizer

$$C(a) = \{g \in G \mid g^{-1} a g = a\}$$

for subgroups instead of elements.

Note 25.5: $N(A)$ is the set of elements $g \in G$ with respect to which A is normal.

Theorem 25.6
For all subgroups $A \subseteq G$:

1. $N(A)$ is a subgroup of G.
2. $A \lhd N(A)$.

Proof. Follows directly from the definition of $N(A)$. □

Definition 25.7
Let $[A]_H$ denote the class of all subgroups of G that are H-conjugate to A, i.e. $[A]_H =$ equivalence class of A under H-conjugation.

Theorem 25.8
Suppose $|G| < \infty$, and H is a fixed subgroup of G.

$$\Big|[A]_H\Big| = [H\colon H \cap N(A)]$$

Compare it with $\Big|[a]\Big| = [G\colon C(a)]$

Proof. Proof is analogous to the proof of $\Big|[a]\Big| = [G\colon C(a)]$ in the case of elements instead of subgroups. □

Lemma 25.9
Suppose Q is a sylow p-subgroup of G with $|G| < \infty$. If $x \in G$ with $|x| = p^r$ for some $r \in \mathbb{N}$, and $x^{-1}Qx = Q \implies x \in Q$.

Proof. If $x^{-1}Qx = Q \implies x \in N(Q)$.

$$Q \lhd N(Q) \implies N(Q)/Q \text{ is well defined}$$

Consider $Qx \in N(Q)/Q$

$$|x| = p^r \implies |Qx| = p^r$$

Consider

$$\langle Qx \rangle \subseteq N(Q)/Q \text{ with } |\langle Qx \rangle| = p^r$$

By Correspondence Theorem $\implies$ there exists subgroup $Q \subseteq H \subseteq N(Q)$ such that $H/Q = \langle Qx \rangle$. By Lagrange

$$\implies |H| = |\langle Qx \rangle| \cdot |Q| = p^r p^n = p^{n+r}$$

which contradicts Q being a Sylow p-subgroup.

$$r = 0 \implies |\langle Qx \rangle| = p^0 = 1 \implies |H|/|Q| = 1 \implies |H| = |Q| \implies Q \subseteq H \implies H = Q$$

And

$$\langle Qx \rangle = H/Q = \langle e \rangle = Q \implies Qx = Q \implies x \in Q$$

□

25.2 Second-Sylow Theorem

Theorem 25.10 (Second-Sylow Theorem)
Suppose $|G| < \infty$. If K and P are two Sylow-p-subgroups of G, then there exists $x \in G$ such that $P = x^{-1}Kx$. Hence any two Sylow p-subgroups are isomorphic.

Proof. Suppose $|K| = |P| = p^n$ where $p \Big| |G|$. Let $K_1, \ldots, K_t$ denote distinct conjugates of K, so $|K_i| = p^n$ for all i. By previous theorem $t = [G\colon N(K)]$. Since $K_i = x^{-1}Kx$ and

$K_j = y^{-1}Ky$ for some $x, y \in G$

$$\implies K_j = y^{-1}(xK_ix^{-1})y = (x^{-1}y)^{-1}K_i(x^{-1}y)$$

$\implies$ every K_j is conjugate to K_i.
We will continue the proof in the next lecture. $\square$