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 nxn 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:

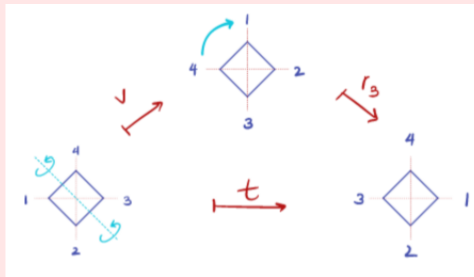
- $\det(A+B) \neq \det(A) + \det(B)$
- $\det(AB) = \det(A) \cdot \det(B)$

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.

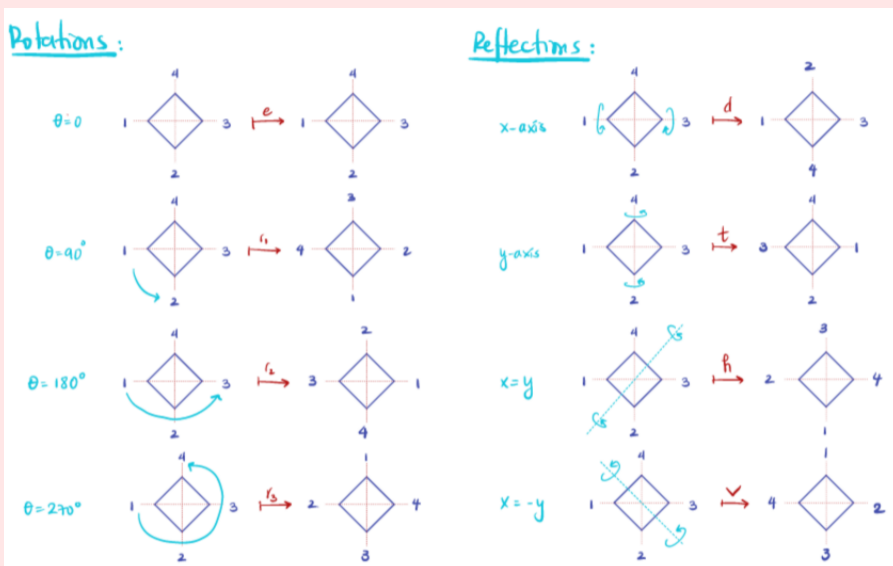
2.2 Symmetries

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 <u>Dihedral Group of degree 4</u>, denoted D_4.

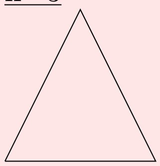
$$D_4 = \{r_1, r_2, r_3, r_4, d, t, h, v \mid \text{under } \circ\}$$



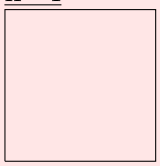
These are Professor Gonzales's lovely drawings.

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

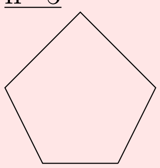
- n=3



- 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 $\{1,2,3\}$

$$e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \tau_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \tau_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$
$$\tau_{21} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \tau_{12} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \tau_{121} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

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

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:

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

Side note: $(S, ☺)$
$☺ : S \times S \to S \implies S$ 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
$\mathbb{Z}_n \times \mathbb{Z}_m \quad n, m \in \mathbb{N}$.
$(a, b) \,\square\, (a', b') = (\underbrace{a + a'}_{\text{mod } n}, \underbrace{b + b'}_{\text{mod } m})$

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

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 $a^{-1} \in G$
   $$\begin{aligned} \implies \underbrace{a^{-1}a}_{e} b &= \underbrace{a^{-1}a}_{e} c \\ \implies e \cdot b &= e \cdot c \\ \implies b &= c \end{aligned}$$
3. Suppose $a \in G$ $\exists$ two distinct inverses.
   $d_1, d_2 \in G$.
   $d_1 a = e = a d_1$
   $d_2 a = e = a d_2$
   $\implies d_1 = d_1 e = d_1 a d_2 = e \cdot d_2 = d_2$

$\square$

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; $e, \tau_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$|e| = 1; e^1 = e$
$|\tau_1| = 2 \quad \tau_1^2 = \tau_1 \circ \tau_1 = e$
$\tau_1^4 = \tau_1^2 \circ \tau_1^2 = e \circ e = e$

Example 3.10
$\mathbb{Z} \leftarrow e = 0$.
$|1| = ?$
$1 \cdot n = 0$ for which n?
Answer none!
$\implies |1| = \infty$

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

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 $|a| < \infty$ $\forall a \in G$. Suppose $c \in G$ such that $|a| \leq |c|$ $\forall a \in G$. 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,

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

<u>Note:</u> $|a| = n, |b| = m, |a \cdot b| \neq n \cdot m$ unless $(n, m) = 1$
<u>Recall:</u> $|c| = p^s \cdot n$ 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 <u>subgroup</u> of $(G, *)$ if it is also a group under $*$.
<u>Note:</u>
$G \subseteq G \implies G$ 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 <u>nontrivial proper subgroup</u>.

Examples 4.5

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

<u>Note:</u> 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 $n \in \mathbb{N}$.
$\implies a^n = e$
$\implies a^{n-1} \cdot a = e = a \cdot a^{n-1}$
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.
$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$\tau_2 e = \tau_2 = e\tau_2 \implies \underbrace{\{e, \tau_2\}}_{H}$ is closed.
$\tau_2 \cdot \tau_2 = e$
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 center 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. $a \in Z(G), ag = ga \quad \forall g \in G.$
   $\implies a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$
   $\implies ga^{-1} = a^{-1}g \implies a^{-1} \in Z(G)$

□

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

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 ($|a| < |c| \quad \forall a \in G$). 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.

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

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

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

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

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

□

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 product of all elements of S and their inverses.

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

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

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

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 $n!$

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

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

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

$\mathbb{Z}_8 = \{0, \ldots, 7\}$

$\mathcal{U}_8$ 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