Math 113
Abstract Algebra

Kelvin Lee

UC Berkeley

Contents

Chapter 1

Sets and Relations

1.1 Sets

Definition 1.1.1 (Subset)**.** A set A is a **subset** of a set B if $x \in A \implies x \in B$. We write $A \subseteq B$ or $A \subset B$.

Definition 1.1.2 (Proper subset)**.** A **proper subset** is $A \subseteq B$ but $A \neq B$, i.e., $A \subset B$.

Remark. $A = B$ is equivalent to saying that $A \subseteq B$ and $B \subseteq A$.

1.2 Set Operations

Definition 1.2.1 (Union)**.** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

Definition 1.2.2 (Intersection)**.** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

Definition 1.2.3 (Difference)**.** $A \backslash B = A - B = \{a \in A \mid a \notin B\}$.

Definition 1.2.4 (Cartesian product)**.** $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Remark. $A \times B \neq B \times A$.

Definition 1.2.5 (Complement)**.** The **complement** of $A \subseteq U$ is $A^c = \{a \in U \mid a \notin A\}$ where U is the universe.

Remark. $A \cup A^c = U$; $A \cap A^c = \emptyset$; $(A^c)^c = A$.

Theorem 1.2.6 (De Morgan's Laws)**.**

$$(A \cup B)^c = A^c \cap B^c,$$

$$(A \cap B)^c = A^c \cup B^c.$$

1.3 Relations

Definition 1.3.1 (Relations)**.** A **relation** between sets A and B is a subset $\mathcal{R} \subseteq A \times B$. If $(a, b) \in \mathcal{R}$, then a is related to b, or $a\mathcal{R}b$, or $a \sim b$.

Example 1.3.2. $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R}$. $\mathcal{R} = \{(x, x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$, i.e., $a\mathcal{R}b \iff f(a) = b$, where $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = x$.

Example 1.3.3. $\mathcal{R} \subseteq \mathbb{R}^2$, $a\mathcal{R}b \iff b = a^3$, i.e., $\mathcal{R} = \{(x, x^3) \mid x \in \mathbb{R}\}$.

1.3.1 Functions

Definition 1.3.4 (Function)**.** A **function** $f : A \to B$ is a relation $\mathcal{R} \subseteq A \times B$ such that $\forall a \in A, \exists! b \in B$ such that $(a, b) \in \mathcal{R}$.

Definition 1.3.5 (Binary Operation)**.** A **binary operation** on a set A is a function $f : A \times A \to A$.

Definition 1.3.6 (Disjoint)**.** $A, B \subseteq U$ are **disjoint** if $A \cap B = \emptyset$.

Definition 1.3.7 (Partition)**.** A **partition** of U is a collection of disjoint subsets of U whose union is U.

Example 1.3.8. $U = \mathbb{Z}$ can be partitioned into $\{x \in \mathbb{Z} \mid x < 0\}, \{x \in \mathbb{Z} \mid x > 0\}$.

Example 1.3.9. $U = \mathbb{R}$ can be partitioned by the sets $\{x\}$ for each $x \in \mathbb{R}$.

Definition 1.3.10 (Equivalence Relation)**.** A relation $\mathcal{R} \subseteq A \times A$ is an **equivalence relation** if it is

(i) **reflexive**: $a\mathcal{R}a \quad \forall a \in A$.

(ii) **symmetric**: $a\mathcal{R}b \iff b\mathcal{R}a$.

(iii) **transitive**: $a\mathcal{R}b$ and $b\mathcal{R}c \implies a\mathcal{R}c$.

Remark. Equivalence relation "are the same" as partition, i.e., they contain the same information. (Why)?

- If $\mathcal{R}$ is an equivalence relation on A, then create partition of A: say a and b are in the same subset of the partition $\iff a\mathcal{R}b$. This is a partition of A.
- Given a partition of A, make a relation $\mathcal{R}$ on A by saying $a\mathcal{R}b \iff a$ and b are in the same subset of the partition. Check $\mathcal{R}$ is an equivalence relation.

Example 1.3.11. If $\mathbb{Z}$ are partitioned into $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ for some $n2$, the corresponding equivalence relation is *congruence modulo n*. For $a\mathcal{R}b$, write $a \equiv b \pmod{n}$.

1.4 Modular Arithmetic

Notation.

$$\overline{i} = \{x \in \mathbb{Z} \mid i \text{ is the remainder when } x \text{ is divided by } n\} = \{an + i \mid a \in \mathbb{Z}\}.$$

Define $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Goal is to define $+$ and $\times$ on $\mathbb{Z}_n$.

To do so, first, given $x \in \mathbb{Z}$, let $\overline{x} = \{an + x \mid a \in \mathbb{Z}\}$. Then $\overline{x} = \overline{y}$ when $x - y = kn$ for some $k \in \mathbb{Z}$, i.e., $x - y \in \overline{0}$. Now for $+/\times$: define $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{a+b}$ and define $\times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{ab}$.

Question. Define $\overline{a} + \overline{b} = \overline{a+b}$. But if $\overline{a} = \overline{x}$ and $\overline{b} = \overline{y}$, then is $\overline{a+b} = \overline{x+y}$?

Question. Write out tables of binary operations for $n = 3$.

Chapter 2

Groups

2.1 Properties of $+$ on $\mathbb{R}$ and $\times$ on $\mathbb{R}\backslash\{0\}$

(i) **Closure**: adding/ multiplying two elements gives another element (built in to definition of a binary operation).

(ii) **Commutativity**:

$$\begin{cases} a+b &= b+a \\ ab &= ba \end{cases} \quad \forall a, b.$$

(iii) **Associativity**

$$\begin{cases} a+(b+c) &= (a+b)+c \\ a(bc) &= (ab)c \end{cases} \quad \forall a, b, c.$$

(iv) **Identity**

$$\begin{cases} a+0 &= 0+a = a \\ a\cdot 1 &= 1\cdot a = a \end{cases} \quad \forall a.$$

(v) **Inverses**

$$\begin{cases} a+(-a) &= 0 \\ a\cdot \frac{1}{a} &= 1 \end{cases} \quad \forall a.$$

Definition 2.1.1. We say a binary operation $p : A\times A \to A$ is:

- **commutative** if $p(a,b) = p(b,a) \quad \forall a, b \in A$.
- **associative** if $p(a,p(b,c)) = p(p(a,b),c) \quad \forall a, b, c \in A$.
- **has an identity** if $\exists e \in A$ such that $p(a,e) = p(e,a) = a \quad \forall a \in A$.
- **has inverses** if $\exists$ identity $e \in A$ and $\forall a \in A, \exists b \in A$ such that $p(a,b) = p(b,a) = e$. We denote the inverse as a^{-1}.

Example 2.1.2. $A = \mathbb{Z}_n, p =$ addition mod n, i.e., $p(i,j) = \bar{i} + \bar{j}$.

1. **Associativity:**

$$\begin{aligned}\bar{i} + (\bar{j} + \bar{k}) = \bar{i} + \overline{j+k} &= \overline{i + (j+k)} \\ &= \overline{(i+j)+k} \\ &= \overline{i+j} + \bar{k} \\ &= (\bar{i} + \bar{j}) + \bar{k}.\end{aligned}$$

2. **Identity:** $\bar{0}$.
3. **Inverses:** $\bar{i}$ has inverse $\overline{-i} = \overline{n-i}$. (e.g. $n = 2$: inverse of $\bar{1} = \overline{-1} = \overline{2-1} = \bar{1}$.
4. **Commutativity:**

$$\bar{i} + \bar{j} = \overline{i+j} = \overline{j+i} = \bar{j} + \bar{i}.$$

Example 2.1.3. $A = \text{Mat}_n(\mathbb{R})$ = set of $n \times n$ matrices with entries in $\mathbb{R}$. $p : A \times A \to A$ is matrix multiplication. **Associativity:** matrix multiplication is associative. **Identity:** I_n the identity matrix. **Inverses:** No, consider the inverse for the zero matrix. **Commutativity:** $AB \neq BA$ for matrices.

Example 2.1.4. $A = GL_n(\mathbb{R})$ General linear group (invertible matrices). **Associativity:** yes. **Identity:** yes. **Inverses:** yes. **Commutativity:** no.

Example 2.1.5. A = set of functions $f : \mathbb{R} \to \mathbb{R}, p(f, g) = f \circ g$. **Associativity:** yes. **Identity**: $f(x) = x$. **Inverses**:? **Commutativity:** no, e.g.?

2.1.1 Properties

- If p is a binary operation on A with identity e, and $ab = ac = e$ and $ba = ca = e$. (ab means $p(a, b)$, ac means $p(a, c)$), then $b = c$. This is the **cancellation law**.

  Remark. (Why?) $ab = e \implies cab = ce \implies eb = c \implies b = c$. Hence, inverses are *unique*. That is, if $e, f \in A$ are such that

  $$\begin{cases} ea = ae &= a \\ fa = af &= a \end{cases} \quad \forall a \in A,$$

  then $e = f$.
  (Why?) $e = ef = f$ (f, e is identity).

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

Definition 2.1.6 (Groups)**.** A **group** is a set G with a binary operation $p : G \times G \to G$ that is *associative*, *has an identity* e, and *has inverses.* Write this as (G, p) or just G if the binary operation is understood from context.

Definition 2.1.7 (Abelian)**.** A group (G, p) is **Abelian** or **communitative** if p is commutative.

Notation: write $p(a, b)$ as ab or $a + b$ sometimes depending on the context.

Remark. Some authors have four properties: with the extra one being **closure**. For us, closure is built in to the definition of p.

Example 2.1.8. Examples of Abelian group:$(\mathbb{R},+)$,$(\mathbb{R}\backslash\{0\},\times)$, $(\mathbb{Z}_n,+)$.
Examples of non-Abelian group: $(GL_n(\mathbb{R}),\times)$.
Examples of non-group: $(\mathrm{Mat}_n(\mathbb{R}),\times)$, $(\{f:\mathbb{R}\to RR\},\text{commposition})$, $(\mathbb{N},+)$.

Definition 2.1.9 (Order)**.** The **order** of a group is the cardinality of G as a set.

Notation: $|G|$ = order of G. $|\mathbb{R}|=\infty, |\mathbb{Z}_n|=n$.

Theorem 2.1.10 (Cancellation Law)**.** *In a group G, if $ab=ac$, then $b=c$, i.e., we can cancel a.*

Proof. a has inverse $a^{-1}\in G$. Hence,

$$ab=ac \implies a^{-1}ab=a^{-1}ac \implies eb=ec \implies b=c.$$

□

Example 2.1.11.

- $GL_n(\mathbb{R}), GL_n(\mathbb{C}), GL_n(\mathbb{Q})$ under matrix multiplication. (*General linear groups*)

- $SL_n(\mathbb{R}), SL_n(\mathbb{C}), SL_n(\mathbb{Q})$ under matrix multiplication. (*Special linear groups*, i.e. $SL_n(\mathbb{R})=\{A\in GL_n(\mathbb{R})\mid \det A=1\}$.) Matrix multiplication can be reimagined as a binary operation $SL_n(\mathbb{R})\times SL_n(\mathbb{R})\to SL_n(\mathbb{R})$.

- Given a set $[n]=\{1,2,\dots,n\}$, let S_n = set of bijections $[n]\to[n]$. For example, $f:[3]\to[3]$ $(f(1)=1, f(2)=3, f(2)=3)$ is an element of S_3. Define binary operation p on S_3 by function composition $fg=f\circ g$, e.g. $(fg)(1)=(f\circ g)(1)=f(g(1))$. This forms a group (S_n,p), called the **symmetric group**, e.g. for f above: $f\circ f$ is $(1\to1, 2\to2, 3\to3)$, which is the identity function.

  Remark. It is a group. **Associativity:** function composition is associative. **Identity:** $f(i)=i\quad\forall i$. **Inverse:** every bijection has an inverse bijection (if $f(i)=j$, then define $f^{-1}(j)=i$) and so $f\circ f^{-1}=f^{-1}\circ f=e$. Hence, S_n is a group.
  These bijection can be thought of as permutations of the list $\{1,2,\dots,n\}$, e.g. f above permutes 123 to 132. It also permutes 132 to 123. f takes the second slot to third slot and the third slot to second slot. f permutes: $123\overset{f}{\rightsquigarrow}132\overset{f}{\rightsquigarrow}123$. There are $n!$ different permutations of $123\cdots n$ and so $|S_n|=n!$.

2.2 Subgroups

Definition 2.2.1 (Subgroup)**.** A **subgroup** is a non-empty subset H of a group (G,p) such that

- H is closed under p: $p(a,b)\in H\quad\forall a,b\in H$.

- H has inverses: if $a\in H$, then $a^{-1}\in H$.

Under these conditions, we can define a new binary operation: $p_H: H\times H\to H$ defined by $p_H(a,b)=p(a,b)$.

Proposition 2.2.2. (H,p_H) is a group.

Proof. p_H is a well-defined binary operation since H is closed under p. We also have the identity $e \in H$ since given any $a \in H$, we know that $a^{-1} \in H$. Hence, we have $p_H(a, a^{-1}) = p(a, a^{-1}) = e \in H$. The inverse is also given. For associativity, we have p_H is associative because p is associative. □

Notation: $H \leq G$ means H is a subgroup of G.

Example 2.2.3. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Example 2.2.4. $(\mathbb{Q}\backslash\{0\}, \times) \leq (\mathbb{R}\backslash\{0\}, \times) \leq (\mathbb{C}\backslash\{0\}, \times)$.

Remark. Examples of non-subgroups: $(\mathbb{R}\backslash\{0\}, \times) \not\leq (\mathbb{R}, +)$, $(\mathbb{R}\backslash\{0\}, +) \not\leq (\mathbb{R}, +)$

Example 2.2.5. $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ (under matrix multiplication).

Example 2.2.6. For any group G, $\{e\} \leq G$, called the **trivial subgroup**.

Definition 2.2.7 (Proper Subgroup)**.** A subgroup $H \leq G$ is a **proper subgroup** if $H \neq G$.

2.2.1 Subgroups of $(\mathbb{Z}, +)$

Let $a \in \mathbb{Z}$ and define $a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$ (multiples of a).

Proposition 2.2.8. $(a\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ for any $a \in \mathbb{Z}$.

Proof. Non-emptiness: $a \in a\mathbb{Z}$, so $a\mathbb{Z} \neq \emptyset$. Closure: given $ax, ay \in a\mathbb{Z}$, we want to check that $ax + ay \in a\mathbb{Z}$. But $ax + ay = a(x + y) \in a\mathbb{Z}$. Inverses: given $ax \in a\mathbb{Z}$, we know that $a(-x) \in a\mathbb{Z}$ and $ax + a(-x) = ax - ax = 0$, so $a(-x)$ is the inverse of ax and thus $a\mathbb{Z}$ has inverse. □

Theorem 2.2.9. *If $H \leq \mathbb{Z}$, then $H = a\mathbb{Z}$ for some $a \in \mathbb{Z}$.*

Proof. Since $H \leq \mathbb{Z}$, $0 \in H$ (identity). If $H = \{0\}$. then $H = 0\mathbb{Z}$ and we are done. If not, let a be the smallest positive integer in H (see explanation in the following remark). To show that $H = a\mathbb{Z}$, we need to show that $H \subseteq a\mathbb{Z}$ and $a\mathbb{Z} \subseteq H$.
$\underline{(a\mathbb{Z} \subseteq H)}$: given any $ax \in a\mathbb{Z}$, we have

$$ax = \begin{cases} \underbrace{a + \cdots + a}_{x} & \text{if } x > 0, \\ \underbrace{(-a) + \cdots + (-a) + \cdots}_{x} & \text{if } x < 0, \\ 0 & \text{if } x = 0. \end{cases}$$

When $x > 0$, $ax \in H$ since H is closed under addition. When $x < 0$, $ax \in H$ as $-a \in H$ since H has inverse and H is closed under addition. When $x = 0$, $ax \in H$ since H has identity. Hence, since for all cases we have $ax \in H$, this shows that $a\mathbb{Z} \subseteq H$.
$\underline{(H \subseteq a\mathbb{Z})}$: let $b \in H$, write $b = ax + r$ for some $r, x \in \mathbb{Z}$ with $r \in \{0, 1, \ldots, a - 1\}$. Note that $r = b + a(-x) \in H$ since $b \in H, a(-x) \in a\mathbb{Z} \subseteq H$ and H is closed under addition. If $r \neq 0$, then r is a positive integer in H smaller than a. But this contradicts our choice of a as the smallest positive integer in H. Hence, $r = 0$, and $b = ax \in a\mathbb{Z}$. Hence, $H \subseteq a\mathbb{Z}$.
Therefore, we conclude that $H = a\mathbb{Z}$. □

Remark. For the second case, H contains a positive integer! (Why?) If not, then H only contains 0 and negative numbers, but then H has no inverses.

Given $a\mathbb{Z}, b\mathbb{Z} \neq \{0\}$, we can define $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$. As an exercise, show that this is a subgroup of $\mathbb{Z}$. Assuming that we have proved the claim, then by the theorem above, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$ and we can take $d > 0$.

Definition 2.2.10 (Greatest Common Divisor)**.** If $a \neq 0, b \neq 0$, then d is the **greatest common divisor** of a and b. We write $d = gcd(a, b)$.

Proposition 2.2.11. If $a \neq 0, b \neq 0$, $d = gcd(a, b)$, then:

(i) $d|a$ and $d|b$,

(ii) if $e|a$ and $e|b$, then $e|d$,

(iii) $\exists x, y \in Z$ such that $ax + by = d$.

Proof. Recall that $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

(i) (1) $a \cdot 1 + b \cdot 0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, so $a \in d\mathbb{Z} \implies a$ is a multiple of $d \implies d|a$.

(2) $a \cdot 0 + b \cdot 1 \in d\mathbb{Z}$, so $b \in d\mathbb{Z} \implies b$ is a multiple of $d \implies d|b$.

(ii) if $e|a$ and $e|b$, then $e|ax + by = d$.

(iii) $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, so $\exists x, y \in \mathbb{Z}$ such that $d = ax + by \in a\mathbb{Z} + b\mathbb{Z}$.

□

Remark. If $ax + by = n$, it is now always the case that $n = gcd(a, b)$. For example, $gcd(2, 4) = 2$, but $2 \cdot 2 + 4 \cdot 1 = 8 \neq gcd(2, 4)$.

Definition 2.2.12. $a, b \in \mathbb{Z}$ are **relatively prime** if $gcd(a, b) = 1$.

Remark. $gcd(a, b) = 1 \iff \exists x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proposition 2.2.13. If $p \in \mathbb{Z}$ is prime, then $p|ab$ implies $p|a$ or $p|b$.

Proof. If $p|ab$, and $p \nmid a$, we want to show $p|b$. Since p has divisors ± 1 and $\pm p$, then $gcd(a, p) = 1$ or p. But $p \nmid a$ by assumption, so $gcd(a, p) = 1$. Hence, there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Then multiply both sides by b: $abx + pby = b$. Since $p|ab$ and $p|p$, $p|abx + pby = b$ as required. □

2.2.2 Cyclic subgroups

Definition 2.2.14 (Cyclic subgroups)**.** Let G be a group, $a \in G$. Then

$$\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}.$$

is called the **cyclic subgroup** of G generated by a.

Remark. $\langle a \rangle$ is the smallest subgroup of G containing a, i.e., if $H \leq G$ and $a \in H$, then $\langle a \rangle \subseteq H$ by closure and inverses.

Example 2.2.15. If $f \in S_1$ is $f = (12)(3)$, then $\langle f \rangle = \{e, f\}$.

Definition 2.2.16 (Order)**.** If $\langle a\rangle \leq G$ is finite, let $n \in \mathbb{N}$ be the smallest positive integer such that $a^n = e$. This n is called the **order** of a, written $|a|$. If $|\langle a\rangle| = \infty$, then $|a| = \infty$, and we say that a has **infinite order**.

Proposition 2.2.17. Let $|a| = n < \infty$.

(i) $a^\ell = a^m \iff \ell - m \equiv 0 \pmod n$. In particular, $a^\ell = e \iff \ell \equiv 0 \pmod n$.

(ii) $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $|\langle a\rangle| = n$.

Proof.

(i) If $a^\ell = a^m$, then $a^\ell a^{-m} = a^m a^{-m} \implies a^{\ell-m} = e$. Write $\ell - m = nk + r$ for some $r \in \{0, 1, \ldots, n-1\}$. Then $a^r = a^{(\ell-m)-nk} = a^{\ell-m}(a^n)^{-k} = e \cdot e^{-k} = e$. If $r \neq 0$, then $a^r = e$, but $r < n$. This contradicts the definition of n as the order of a. Hence, $r = 0$ and $\ell - m = nk \implies \ell - m \equiv 0 \pmod n$. Conversely, if $\ell - m \equiv 0 \pmod n$, then $\ell - m = nk$ for some k, so $a^{\ell-m} = (a^n)^k = e^k = e$.

(ii) Exercise. (See book)

□

Exercise 2.2.18. If $|a| = n$, and $\ell \in \{0, \ldots, n-1\}$, then

- $|a^\ell| = 1 \iff \ell = 0$,
- if $d = gcd(n, \ell)$, then $|a^\ell| = \frac{n}{d}$.

Definition 2.2.19 (Cyclic group)**.** A group G is **cyclic** if $\exists a \in G$ such that $G = \langle a\rangle$. We call a a *generator* of G and say that G is generated by a.

Example 2.2.20. $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$, called an *infinite cyclic group.* $\mathbb{Z}_n = \langle \overline{1}\rangle$ for any n, called a *cyclic group of order n.*

2.2.3 Homomorphisms

Definition 2.2.21 (Homomorphism)**.** Given groups (G, p) and (G', p'), a **homomorphism** $\varphi : G \to G'$ is a function such that

$$\varphi(p(a, b)) = p'(\varphi(a), \varphi(b)) \quad \forall a, b \in G.$$

Remark. The point of a group homomorphism is to preserve the structure of the group. The idea is that it doesn't matter whether you multiply first then apply the map or apply the map then multiply. This is what we mean when we say it "preserves the structure" of the group.

Example 2.2.22. $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ and $\varphi(x) = \overline{x}$. To check if this is a homomorphism, we check if $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\forall x, y \in \mathbb{Z}$.

$$\begin{aligned} \varphi(x + y) &= \overline{x + y} \\ \varphi(x) + \varphi(y) &= \overline{x} + \overline{y}. \end{aligned}$$

Since $\overline{x + y} = \overline{x} + \overline{y}$ by definition of $+$ in $\mathbb{Z}_n$, φ is a homomorphism.

Example 2.2.23. $\varphi_k : \mathbb{Z} \to \mathbb{Z}$, $\varphi_k(x) = kx$.

$$\varphi(x + y) = k(x + y) = kx + ky = \varphi(x) + \varphi(y).$$

Hence, it is a homomorphism.

Example 2.2.24. $\exp : (\mathbb{R}, +) \to (\mathbb{R}\backslash\{0\}, \times)$, $\exp(x) = e^x$.

$$\exp(x + y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

Remark. Non-homomorphism example: $\exp : (\mathbb{Q}, +) \to (\mathbb{Q}\backslash\{0\}, \times)$. This is not well-defined since e^x is generally not rational.

Example 2.2.25. $\det : GL_n(\mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$. $\det(AB) = \det(A)\det(B)$.

Example 2.2.26. Given any group G, and any element $a \in G$, define $\varphi : (\mathbb{Z}, +) \to G$, $\varphi(x) = a^x$. Same as for exp. The image of φ is $\langle a \rangle$.

Example 2.2.27. Let G and G' be any groups and let $\varphi : G \to G'$ be defined by $a \rightsquigarrow e_{G'}$, $\forall a \in G$. We have $\varphi(ab) = e_{G'}$ and $\varphi(a)\varphi(b) = e_{G'} \cdot e_{G'} = e_{G'}$. This is called the *trivial homomorphism.*

2.2.4 Properties of Homomorphism

Proposition 2.2.28. If $\varphi : G \to G'$ is a homomorphism, then

(i) $\varphi(a_1, \dots, a_n) = \varphi(a_1)\varphi(a_2) \cdots \varphi(a_n)$.

(ii) $\varphi(e_G) = e_{G'}$.

(iii) $\varphi(a^{-1}) = \varphi(a)^{-1} \quad \forall a \in G$.

Proof.

(i) Induction on definition of homomorphism.

(ii) Since $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G)\varphi(e_G)$, we then multiply both sides by $\varphi(e_G)^{-1}$:

$$\underbrace{\varphi(e_G)^{-1}\varphi(e_G)}_{e_{G'}} = \underbrace{\varphi(e_G)^{-1}\varphi(e_G)}_{e_{G'}}\varphi(e_G) \implies e_{G'} = e_{G'}\varphi(e_G) = \varphi(e_G).$$

(iii) Given $a \in G$. By (ii), we have

$$\varphi(a \cdot a^{-1}) = \varphi(e_G) = e_{G'}.$$

Since φ is a homomorphism,

$$\varphi(a \cdot a^{-1}) = \varphi(a)\varphi(a^{-1}) = e_{G'},$$

which implies that $\varphi(a^{-1}) = \varphi(a)^{-1}$.

□

Remark.

(1) The image of φ is $\varphi(G) = \{\varphi(a) \mid a \in G\} \subseteq G'$. $\varphi(G)$ is a subgroup of G'.

(2) The kernel of φ is $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_{G'}\} \subseteq G$. $\ker(\varphi)$ is a subgroup of G.

Proof.

(1) *Closure*: if $\varphi(a), \varphi(b) \in \varphi(G)$, then $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(G)$. *Inverses*: if $\varphi(a) \in \varphi(G)$, then $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(G)$.

(2) *Closure*: if $a, b \in \ker(\varphi)$, then

$$\varphi(ab) = \varphi(a)\varphi(b) = e_{G'}e_{G'} = e_{G'} \implies ab \in \ker(\varphi).$$

Inverses: if $a \in \ker(\varphi)$, then

$$\varphi(a^{-1}) = \varphi(a)^{-1} = e_{G'}^{-1} = e_{G'} \implies a^{-1} \in \ker(\varphi).$$

□

Example 2.2.29. $\det : GL_n(\mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$. The identity of $(\mathbb{R}\backslash\{0\}, \times)$ is 1, so

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = SL_n(\mathbb{R}).$$

Proposition 2.2.30. If $\varphi : G \to G'$ is a homomorphism, then φ is injective if and only if $\ker(\varphi) = \{e_G\}$.

Proof. If φ is injective, and $a \in \ker(\varphi)$, then $\varphi(a) = e_{G'}$. But also $\varphi(e_G) = e_{G'}$. φ being injective implies that $a = e_G$. Hence, $\ker(\varphi) = \{e_G\}$.
Conversely, if $\ker(\varphi) = \{e_G\}$, and $\varphi(a) = \varphi(b)$ for some $a, b \in G$. Multiplying both sides by $\varphi(b)^{-1}$ gives

$$\varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_{G'},$$

which implies that $\varphi(a)\varphi(b^{-1}) = e_{G'} \implies \varphi(ab^{-1}) = e_{G'} \implies ab^{-1} \in \ker(\varphi)$. Since $\ker(\varphi) = \{e_{G'}\}$, we know $ab^{-1} = e_G \implies a = b$. Hence, φ is injective. □

2.2.5 Isomorphisms

Definition 2.2.31 (Isomorphism)**.** An **isomorphism** $\varphi : G \to G'$ is a bijective homomorphism.

Example 2.2.32. $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is an isomorphism.

Remark. If $\varphi : G \to G'$ is an injective homomorphism, then $\varphi : G \to \varphi(G) \leq G'$ is an isomorphism.

Example 2.2.33. Let $\varphi : (\mathbb{Z}, +) \to \langle a \rangle \leq G$ be defined by $x \rightsquigarrow a^x$ for some $a \in G$. φ is surjective. φ is injective if and only if a has infinite order. If $|a| = n$, then $\varphi : (\mathbb{Z}_n, +) \to \langle a \rangle \leq G$ defined by $\overline{x} \rightsquigarrow a^x$ is an isomorphism.

Example 2.2.34. Given $A \in GL_n(\mathbb{R})$, the map $f_A : (\mathbb{R}^n, +) \to (\mathbb{R}^n, +)$ defined by $\vec{v} \rightsquigarrow A\vec{v}$ is an isomorphism. *Homomorphism*: $f_A(\vec{v} + \vec{w}) = A(\vec{v} + \vec{w}) = A\vec{v} + A\vec{w} = f_A(\vec{v}) + f_A(\vec{w})$. *Bijection*: Since A is invertible, $\exists$ inverse matrix $A^{-1} \in GL_n(\mathbb{R})$. Then $f_{A^{-1}}$ is the inverse function to f_A, i.e., $f_A \circ f_{A^{-1}} = f_{A^{-1}} \circ f_A = id_{\mathbb{R}^n}$. Any invertible function is a bijection.

Example 2.2.35. If $a \in G$, then the map $\varphi_a : G \to G$ defined by $b \rightsquigarrow aba^{-1}$ is an isomorphism. This is called *conjugation by* a, and aba^{-1} is the conjugate of b by a.

Exercise 2.2.36. Check $\varphi_a(bc) = \varphi_a(b)\varphi_a(c)$ and check φ_a is a bijection. (Hint: find an inverse function)

Proposition 2.2.37. If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Proof. φ^{-1} exists and is a bijection, as φ is a bijection. Now we show that it is a homomorphism by choosing $x, y \in G'$ and show that $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$. For simplicity, let $\varphi^{-1}(x) = a, \varphi^{-1}(y) = b, \varphi^{-1}(xy) = c$ and we want to show that $c = ab$. Now

$$\begin{aligned} c = ab &\iff \varphi(c) = \varphi(ab) && (\varphi \text{ is a bijection}) \\ &\iff \varphi(c) = \varphi(a)\varphi(b) && (\varphi \text{ is a homomorphism}) \\ &\iff \varphi(\varphi^{-1}(xy)) = \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) \\ &\iff xy = xy. \end{aligned}$$

Thus, $c = ab$, which implies that φ^{-1} is a homomorphism. Since it's also bijective, it's an isomorphism. □

Corollary 2.2.38. The relation $G \sim G' \iff \exists$ isomorphism $G \to G'$ is an equivalence relation.

Proof. Reflexive: $G \sim G$, as $\mathrm{id}_G : G \to G$ is an isomorphism. *Symmetric*: if $G \sim G'$ and $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is an isomorphism, so $G' \sim G$. *Transitive*: if $G \sim G'$, $G' \sim G''$ and $\varphi : G \to G'$, $\varphi' : G' \to G''$ are isomorphisms, then $\varphi' \circ \varphi : G \to G''$ is an isomorphism, so $G \sim G''$. □

Definition 2.2.39. We say G and G' are **isomorphic** if $\exists$ an isomorphism $\varphi : G \to G'$

Notation: $G \cong G'$.

Remark. There is no such notion of "homomorphic".