MATH100A: Abstract Algebra

Course Webpage

October 15, 2021

Abstract

Warning: This is only a piece of lecture notes written by a careless scribe. So just be careful with and tolerant of any possible typos or misunderstandings when you read [0.1]. The scribe does not intend to make anyone to be driven by his stupidity! Also, the professor's explanation is extremely helpful as he discusses a lot about the interpretable ideas behind the dull scripts. So watch the lecture before reading this. If you have any suggestions (e.g. typos, typography, logistics), please do not hesitate contacting the scribe!

Without specifications, the notation use is as the following

- $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \ldots$: real, complex, quadratic, and so on
- $\mathcal{R}$: integrability
- $\mathbb{1}$: characteristic function
- s: simple function
- $\mathcal{F}$: family
- $\mathcal{A}$: algebra

[0.1] Especially '$\cap$' and '$\cup$' are often mistaken because of typos.

Contents

MATH100A **Fall 2021**

Lecture 1: Law of Composition

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Definition 1.1 (*Law of Composition*)

A ***law of composition*** *on set S is a rule for combining two elements $a, b \in S$ to create another element $p \in S$*

$$S \times S \to S$$

e.g.1.

- Addition on $\mathbb{Z}, \mathbb{R}$, etc
- Multiplication on $\mathbb{Z}, \mathbb{R}$, etc
- Cross product: $v_1, v_2 \in \mathbb{R}^3 \to v_1 \times v_2 \in \mathbb{R}^3$
- Dot product is **NOT**: $v_1, v_2 \in \mathbb{R}^3 \to v_1 \cdot v_2 \in \mathbb{R}$
- Division is **NOT**: division by 0 fails
- Composition of functions $f \circ g : t \to f(g(t))$

Definition 1.2 (*Commutative*)

A law of composition is ***commutative*** *if $ab = ba$* [1.1].

Definition 1.3 (*Associative*)

A law of composition is ***associative*** *if $(ab)c = a(bc)$.*

Proposition 1.1

For an associate law of composition on S, there is a unique way to define a product of n elements $a_1, a_2, \ldots, a_n$ temporarily denoted as $[a_1, a_2, \ldots, a_n]$:

1. $[a_1] = a_1$
2. $[a_1, a_2] = a_1 a_2$
3. $\forall 1 \leq i \leq n : [a_1, a_2, \ldots, a_n] = [a_1, \ldots, a_i][a_{i+1}, a_n]$

Proof: By induction, $n = 1, 2$ are defined. Now suppose the proposition holds at $r = n - 1$, then $[a_1, a_2, \ldots, a_n] = [a_1, \ldots, a_{n-1}][a_n] = ([a_1, \ldots, a_i][a_{i+1}, a_{n-1}][a_n]) = [a_1, \ldots, a_i]([a_{i+1}, \ldots a_{n-1}][a_n]) = [a_1, \ldots, a_i][a_{i+1}, \ldots, a_n]$. ∎

[1.1] We commonly use ab to denote laws of composition. $a + b$ is only used for commutative laws in this course.

Definition 1.4 (*Identity*)

*An **identity** of a law of composition is an element $e \in S$ satisfying $\forall a \in S : ea = a = ae$* [1.2].

A law of composition can have at most one identity.

Definition 1.5 (*Invertible*)

*Suppose an associative law of composition on S has an identity 1. An element $a \in S$ is **invertible** if $\exists b \in S : ab = 1 = ba$* [1.3].

Proposition 1.2

1. *If a has both left inverse $la = 1$ and a right inverse $ar = 1$, then $l = r = a^{-1}$.*
2. *Inverses are unique.*
3. $(ab)^{-1} = b^{-1}a^{-1}$

Exercise: Let $T = \{a, b\}, S = \{f : T \to T\}$. Fill the i-τ-α-β table where $i(a) = a, i(b) = b$ (identity map); $\tau(a) = b, \tau(b) = a$ (transposition map); $\alpha(a) = \alpha(b) = a$ (constant function); $\beta(a) = \beta(b) = b$ (constant function).

[1.2] Identities are denoted 1 if compositions are written multiplicatively; 0 if compositions are written additively.

[1.3] If so, we call b the inverse of a and write $b = a^{-1}$, or $-a$ for addition notation.

MATH100A **Fall 2021**

Lecture 2: Group

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Solution to the exercise on the i-τ-α-β table

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

Proposition 2.1

If S has an associative law of composition, then any $a \in S$ has at most one inverse.

Proof: Suppose $b, c \in S$ are both inverses of a. Then $ac = 1 \implies b(ac) = b1 \implies (ba)c = b \implies c = b$. ■

Definition 2.1 (*Group*)

*A **group** is a set G with a law of composition that is*

- *Associative;*
- *Has identity;*
- *Every element has an inverse.*

*A group which is commutative is called an **Abelian group**.*

e.g.1. $(\mathbb{Z}, +)$ is a group.

Definition 2.2 (*Order*)

*The **order** of a group is the number of elements in the set G, $|G|$.*

Proposition 2.2

Let $a, b, c \in G$. If $ab = ac$ or $ba = ca$, then $b = c$.

Proof: $ab = ac \implies a^{-1}ab = a^{-1}ac \implies b = c$. ■

Q&A. $ab = ca \implies b = c$ implies a group is Abelian? Yes.

e.g.2.

1. The $n \times n$ **general linear group**

$$\mathrm{GL}_n = \{n \times n \text{ invertible matrices}\}$$

When $n > 1$, $\mathrm{GL}_n(\mathbb{C}) = \mathbb{C} \setminus \{0\}$; when $n > 1$, then $\mathrm{GL}_n(\mathbb{C})$ is not Abelian.

2. Let T be a set. A bijective map $T \to T$ is called a **permutation** of T. The **symmetric group**

$$\mathrm{Sym}(T) = \{\text{bijections } T \to T\}$$

If $T = \{1, 2, \ldots, n\}$, then we denoted

$$S_n := \mathrm{Sym}(T)$$

And $|S_n| = n!$.

e.g.3.

- $|G| = 1 : G = \{1\}$ is a trivial group.
- $|G| = 2 : G = \{1, g\}$. Then $g^2 = 1$ or $g^2 = g$

Exercise: How many groups of size 3 are there?

e.g.4. S_3 is the smallest non-Abelian group (size 6). Take the cyclic permutation x and the transposition y. Then $x^3 = 1, y^2 = 1, yx = x^2y$. With the cancellation law, elements of $\{1, x, x^2, y, xy, x^2y\}$ are distinct.

Definition 2.3 (*Subgroup*)

*A subset $H \subseteq G$ of a group is a **subgroup** if*

- *Closure:* $\forall a, b \in H : ab \in H$
- *Identity:* $i \in H$
- *Inverses:* $a \in H \implies a^{-1} \in H$

e.g.5. The circle group $\{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of the multiplicative group $(\mathbb{C}, \times)$.

MATH100A **Fall 2021**

Lecture 3: Subgroup $(\mathbb{Z}, +)$

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Multiplication table of S_3 given $G = \{1, a, b\}$

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Let G be a group. Then $\{1\} \subseteq G$ and $G \subseteq G$. These two are called **trivial subgroups**. All other subgroups are called **proper subgroups**.

e.g.1. Subgroups of $\mathbb{Z}$

- $\{0\} \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq \mathbb{Z}$.
- $\{\text{Even numbers}\} \subseteq \mathbb{Z}$.
- $\mathbb{Z}_a := \{n \in \mathbb{Z} : a|n\} \subseteq \mathbb{Z}$.

Theorem 3.1

Let $S \subseteq \mathbb{Z}$ be a subgroups. Then either $S = \{0\}$ or $S = \mathbb{Z}_a$ for a being the minimal positive integer in S [3.1].

Proof: Let $S \subseteq \mathbb{Z}$ be a subgroup. If $S = \{0\}$, we are done. If $S \neq \{0\}$, choose $n \in S : n \neq 0$. So if $n > 0$, then $S \cap \mathbb{Z}_{>0} \neq \emptyset$; if $n < 0$, then $-n \in S : -n > 0$. Thus $S \cap \mathbb{Z}_{>0} \neq \emptyset$. Now we want to show $Z_a = S$. To show $Z_a \subseteq S$, by construction $a \in S$ and $0 \in S$. If $k > 0$, then $ka = a + a + \cdots + a \in S$ by closure under addition; if $k < 0$, then $ka = -a + -a + \cdots + -a \in S$ by $-a \in S$ being the inverse of a and closure. To show $S \subseteq \mathbb{Z}_a$, let $n \in S : n = aq + r$ for $q \in \mathbb{Z}$ and $0 \leq r < a$. Then $-qa \in \mathbb{Z}_a \subseteq S$ and so $r = n + -qa \in S$. Thus either $r = 0$ or $0 < r < a$, contradicting to the minimality of a. ■

Lemma 3.2

- *If $H, K \subseteq G$ are subgroups, then $H \cap K \subseteq G$ is a subgroup.*
- *If $H, K \subseteq G$ are subgroups of an Abelian group, then $H + K = \{h + k : h \in H, k \in K\} \subseteq G$ is a group.*

Proof: The first statement will be a homework and the second is left as exercise. ■

Definition 3.1 (gcd, lcm)

*If $\mathbb{Z}_a + \mathbb{Z}_b = \mathbb{Z}_d$, we define d as the **greatest common divisor** (*gcd*) of a and b to be d. If $\mathbb{Z}_a \cap \mathbb{Z}_b = \mathbb{Z}_m$, we define m as the **least common multiple** (*lcm*).*

[3.1] **Well-ordering Principle**: Every nonempty subset of $\mathbb{N}$ has a minimal element.

Proposition 3.3

Let $a, b \in \mathbb{Z}$ not both be 0 with $d = \gcd(a, b)$. Then

1. *$d|a$ and $d|b$.*
2. *If $e|a$ and $e|b$, then $e|d$.*
3. *$\exists r, s \in \mathbb{Z} : d = ar + bs$.*

Proposition 3.4

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then

1. *$a|m$ and $b|m$.*
2. *If $a|n$ and $b|n$, then $m|n$.*

MATH100A **Fall 2021**

Lecture 4: Cyclic Subgroup

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Lemma 4.1

If $H, K \subseteq G$ are subgroups of an Abelian group G, then $H + K = \{h + k : h \in H, k \in K\}$ is a subgroup of G.

Proof: To check the closure, take $x, y \in H + K$. Then $x = h_1 + k_1$ and $y = h_2 + k_2$ for $h_i \in H$ and $k_i \in K$. Then $x + y = h_1 + k_1 + h_2 + k_2 = (h_1 + h_2) + (k_1 + k_2)$. Since $h_1 + h_2 \in H$ and $k_1 + k_2 \in K$ by subgroups, $x + y \in H + K$.

To check identity, $0 = 0 + 0$ for $0 \in H$ and $0 \in K$.

To check inverses, take $x = h + k$. Then $-x = (-h) + (-k) = -(h + k)$. So $-x \in H + K$. ■

Definition 4.1 (*Relatively Prime*)

*We call $a, b \in \mathbb{Z}$ **relatively prime** if $\mathbb{Z} = \mathbb{Z}_a + \mathbb{Z}_b$, or equivalently $\exists r, s \in \mathbb{Z} : ar + bs = 1$.*

Corollary 4.2

Let p be a prime number (the only positive divisors are 1 and p). If $p|ab$, then $p|a$ or $p|b$.

Proof: Suppose $p|ab$ and $p \nmid a$ so $\gcd(p, a) = 1$. Thus $\exists r, s \in \mathbb{Z} : rp + sa = 1$. Then $rpb + sab = b$ so $p|rpb + sab \implies p|b$. ■

Definition 4.2 (*Cyclic Subgroup*)

*The **cyclic subgroup** of G generated by $x \in G$ is*

$$\langle x \rangle := \{..., x^{-3}.x^{-2}, x^{-1}, 1, x, x^2 \dots .\}$$

$$\text{where } x^k := \begin{cases} xx \dots x & k > 0 \\ x^{-1}x^{-1} \dots x^{-1} & k < 0 \\ 1 & k = 0 \end{cases}$$

Proposition 4.3

If G is a group and $x \in G$, then

1. $x^{r+s} = x^r x^s$
2. $x^{rs} = (x^r)^s$

Proof: Left as exercise (induction). ■

Proposition 4.4

Let $\langle x\rangle$ be a cyclic subgroup of G generated by $x \in G$ and let $S\{k \in \mathbb{Z} : x^k = 1\}$. Then

1. *S is a subgroup of $\mathbb{Z}$.*
2. *$x^r = x^s$ if and only if $x^{r-s} = 1$ i.e. $r - s \in S$.*
3. *Suppose $S \neq \{0\}$ then $S = \mathbb{Z}_n$ and $1, x, x^2, \ldots, x^{n-1}$ are distinct and $|\langle x\rangle| = n$.*

Proof:

1. To check closure, if $n, m \in S$, then $x^n = 1 = x^m$. Then $x^{n+m} = x^n x^m = 1 \cdot 1$. To check identity, $0 \in S$ so $x^0 = 1$. To check inverses, if $n \in S$, then $x^n = 1$. Then $x^{-n} = x^{-1n} = (x^n)^{-1} = 1^{-1} = 1$.
2. $x^r = x^s \iff x^r(x^s)^{-1} = 1 \iff x^r x^{-s} = 1 \iff x^{r-s} = 1$.
3. If $x^r = x^s$ for $0 \leq r < s < n$ then $s - r > 0$ and $x^{s-r} = 1$ by (2) i.e. $s - r \in S$. So $s - r \geq n$ then $n > s \geq s - r \geq n$, contradiction. ∎

e.g.1.

- $|G| = 2$. $|G| = |\langle g\rangle|$.
- $x, y \in S_3$. $x(1) = 2, x(2) = 3, x(3) = 1$, then $|\langle x\rangle| = 3$; $y(1) = 2, y(2) = 2, y(3) = 3$. then $|\langle y\rangle| = 2$.
- $|\mathbb{Z}| = \langle 1\rangle$.
- In $\mathrm{GL}_2(\mathbb{R})$, $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ has infinite order, and $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ has finite order.
- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \langle \overline{1}\rangle$.

MATH100A **Fall 2021**

Lecture 5: Cyclic Subgroup

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Recall: Given $x \in G$, $\langle x \rangle = \{..., x^{-2}, x^{-1}, 1, x, x^2, ...\}$. If $S = \{k \in \mathbb{Z} : x^k = 1\}$, then S is a subgroup of $\mathbb{Z}$. i.e. $S = \{0\}$ or $S = \mathbb{Z}_n$.

e.g.1.

- $\mathbb{Z} = \langle 1 \rangle$.
- $\mathbb{Z}/\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ where $\overline{a}$ is the congruence class of $a \mod n$ and $\overline{a} = \{\text{integers} \equiv a \mod n\} = \{k \in \mathbb{Z} : n | k - a\}$.

Proposition 5.1

Let $x \in G$ with finite order n and let $k = qn + r$ for $0 \leq r < n$. Then

1. *$x^k = x^r$.*
2. *$x^k = 1$ if and only if $r = 0$.*
3. *Let $d = \gcd(k, n)$, then x^k has order $\frac{n}{d}$.*

Proof:

1. $x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = x^r$
2. By (1).
3. By definition, $\left|x^k\right|$ is the smallest positive integer m s.t. $(x^k)^m = 1$. Then $(x^k)^{\frac{n}{d}} = x^{\frac{kn}{d}} = (x^n)^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$. Now to show it is minimum, toward a contradiction, suppose $0 < m < \frac{n}{d}$ such that $(x^k)^m = 1$. Thus by (2), $n | km$ i.e. $km = nq$. So $\frac{k}{d}m = \frac{n}{d}q$ implies that $\frac{k}{d}$ and $\frac{n}{d}$ are coprime. Then $\frac{n}{d} | \frac{k}{d}m \implies \frac{n}{d} | m \implies \frac{n}{d} \leq m$, contradiction. ∎

e.g.2. Suppose x has order $p = 7$. Then x^k has order 7 if $\gcd(k, 7) = 1$ or 1 if $\gcd(k, 7) = 7$. If 7 and k are coprime, then $\langle x \rangle = \langle x^k \rangle$; if $7 | k$, then $x^k = 1$ and $\langle x^k \rangle = \{1\}$.

Exercise: Let x have order 4. Then $\langle x^2 \rangle \subset \langle x \rangle$.

e.g.3. **Klein Four Group** $V_4 = \{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]\}$. Then $|\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \rangle| = 1$. And V_4 is also a subgroup.

e.g.4. **Quaternion Group**: $Q_8 = H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. $H_8 = \{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & 0 \\ 0 & i \end{smallmatrix}\right], \left[\begin{smallmatrix} -i & 0 \\ 0 & -i \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right]\}$.

MATH100A **Fall 2021**

Lecture 6: Cycle

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Definition 6.1 (*Cycle*)

Let f be a bijection. A ***cycle*** *of f is the indices generated by f from some starting point.*

e.g.1. $f \in S_5$: $\begin{array}{c|ccccc} i & 1 & 2 & 3 & 4 & 5 \\ \hline f(i) & 3 & 5 & 1 & 2 & 4 \end{array}$
which can also be denoted as drawn as a graph or $f = (2,5,4)(1,3)$ [6.1] [6.2].

e.g.2. $q = (2,5,4)(1,3)$ and $f = (1,2,3,5)$. Then $q \circ f = (5,1,4,2,3)$

$\begin{array}{c|ccccc} i & 1 & 2 & 3 & 4 & 5 \\ \hline f(i) & 5 & 1 & 4 & 2 & 3 \end{array}$

e.g.3. S_3 is generated by $x = (1,2,3)$ and $y = (1,2)$; it can also be generated by $(1,2),(2,3),(1,3)$.

Facts:

- S_n can be generated by transpositions.
- An n-cycle has order n.
- If $(a,\dots,a_n)$ and $(b,\dots,b_m)$ are disjoint i.e. $a_i \neq b_j$, then they commute.
- If $f = c_1 c_2 \dots c_k$ is a product of disjoint cycles, then $f^m = c_1^m c_2^m \dots c_k^m$.

e.g.4. Find an element of S_5 with order 6.
$f = (1,2,3)(4,5)$ has order 6 because $(4,5)^n = 1 \iff 2|n$ and $(1,2,3)^n = 1 \iff 3|n$. $f = (1,2)(4,6)(3,5)$ has order 2.

Definition 6.2 (*Permutation Matrix*)

The ***Permutation matrix*** *associated to $p \in S_n$ is the $n \times n$ matrix such that*

$$P(\vec{e_i}) = \overrightarrow{e_{P(i)}}$$

e.g.5. $P = (1,2,3)(4,5) \in S_5$ can be described by $P = \begin{bmatrix} 0&0&1&0&0 \\ 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&0&0&1 \\ 0&0&0&1&0 \end{bmatrix}$.

[6.1] $(2,5,4)$ can also be written as $(5,4,2)$ or $(4,2,5)$, but not $(2,4,5)$.
[6.2] We often omit cycle of length 1 in notation so $(1,2)(3)(4,5) = (1,2)(4,5)$.

Proposition 6.1

1. *P has only one element nonzero entry $(a, 1)$ in each row / column.*
2. $\det(P) \in \{\pm 1\}$.
3. *If P, Q are permutation matrices of $p, q \in S_n$, then PQ is the permutation matrix of $pq \in S_n$*

Definition 6.3 (*Sign*)

*The **sign** of $p \in S_n$ is $S_n(p) = \det(P)$.*

Definition 6.4 (*Homomorphism*)

*A **homomorphism** between two groups G and G' is a function*

$$\varphi : G \to G' \quad s.t. \quad \varphi(ab) = \varphi(a)\varphi(b)$$

e.g.6. sgn is a homomorphism as $\operatorname{sgn}(pq) = \det(PQ) = \det(P)\det(Q) = \operatorname{sgn}(p)\operatorname{sgn}(q)$. $\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R}, \times)$ is a homomorphism.

MATH100A **Fall 2021**

Lecture 7: Homomorphism

Lecturer: Kiran Kedlaya *Scribes: Rabbittac*

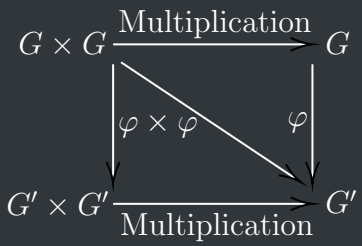

Figure 7.1: commutative diagram of a homomorphism

e.g.1.

- $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$.
- $\mathrm{sgn} : s_n \to \{\pm 1\}$.
- $\exp : \mathbb{R}^+ \to \mathbb{R}^\times$.
- Let G be a group and $a \in G$. The function $\varphi : \mathbb{Z}^+ \to G, \varphi(n) = a^n$ is a homomorphism.

Two generic examples for homomorphisms: For any G, G', we call $\varphi : G \to G', \varphi(a) = 1_{G'}$ **trivial homomorphisms**. For any G and any subgroup $H \subseteq G$, we call $\varphi : H \to G, \varphi(a) = a$ an **inclusion map**.

Proposition 7.1

Let $\varphi : G \to G'$ be a homomorphism. Then

1. $\varphi(a_1, \ldots, a_n) = \varphi(a_1) \ldots \varphi(a_n)$.
2. $\varphi(1_G) = 1_{G'}$.
3. $\forall a \in G : \varphi^{-1}(a) = \varphi(a^{-1})$.

Definition 7.1 (*Isomorphism*)

*An **isomorphism** of G, G' is a homomorphism $\varphi : G \to G'$ which is bijective (on sets). We say G, G' are isomorphic if there exists some isomorphism between them.*

Let $\varphi^{-1} : G' \to G$ be the inverse function. Then φ^{-1} is also a homomorphism. i.e. $\forall a, b \in G' : \varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$. Let $x = \varphi^{-1}(a), y = \varphi^{-1}(b)$. Then $\varphi(xy) = \varphi(x)\varphi(y) \implies xy = \varphi^{-1}(ab)$.

Any "purely structural" property of a group is isomorphism-stable. i.e. If G, G' are isomorphic and G has the property, then so does G'.

e.g.2. Examples of structural properties: finite, order n.

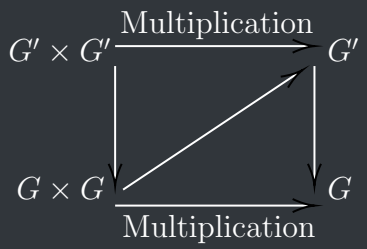

Figure 7.2: commutative diagram of an isomorphism

- Cyclic groups.
- Abelian groups.
- Number of elements of a given order.

Proposition 7.2

Any two cyclic groups of the same order are isomorphic.

Definition 7.2 (*Image*)

Let $\varphi : G \to G'$ be a homomorphism. The ***image*** *of φ is $\operatorname{im}\varphi = \{x \in G' : x = \varphi(a)$ for some $a \in G\}$. The image is a subgroup.*

Proof: $\forall a, b \in G' : \exists x, y \in G : \varphi(x) = a, \varphi(y) = b$. Then $\varphi(xy) = ab$ implies closure. Image has identity. And $\varphi(x^{-1}) = a^{-1}$ shows inverses. ■

e.g.3. Permutation $s_n \to \mathbb{R}^\times$ has image $\{\pm 1\}$.

Definition 7.3 (*Kernel*)

Let $\varphi : G \to G'$ be a homomorphism. The ***kernel*** *of φ is $\ker\varphi = \{a \in G : \varphi(a) = 1_{G'}\}$. The kernel is a subgroup.*

e.g.4. $\varphi = \det$ so $\varphi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. Then $\ker\varphi = \mathrm{SL}_n$ which is the special linear group.

e.g.5. Define $\varphi : S_4 \to S_3$ as follows: S_4 acts on $\{1, 2, 3, 4\}$ which can be divided into two sets of 2 elements into three ways $a = \{\{1, 2\}, \{3, 4\}\}, b = \{\{1, 3\}, \{2, 4\}\}, c = \{\{1, 4\}, \{2, 3\}\}$. Any permutation in S_4 also defines a permutation of $\{a, b, c\}$. Then $\ker\varphi = \{1, (12)(34), (13)(24), (14)(23)\}$.

Definition 7.4 (*Conjugation*)

For any fixed $g \in G$, the function $\varphi : G \to G, \varphi(a) = g^{-1}ag$ is called ***conjugation*** *and is a homomorphism.*

Proof: $\varphi(ab) = g^{-1}abg \implies \varphi(a)\varphi(b) = g^{-1}agg^{-1}bg$. ■

MATH100A **Fall 2021**

Lecture 8: arg2

Lecturer: Kiran Kedlaya *Scribes: Rabbittac*

MATH100A **Fall 2021**

Lecture 9: arg2

Lecturer: Brandon Alberts *Scribes: Rabbittac*

MATH100A **Fall 2021**

Lecture 10: arg2

Lecturer: Brandon Alberts *Scribes: Rabbittac*