4. Groups. Subgroups. Primitive roots.

A. Ushakov

MA503, September 22, 2021

Contents

- Groups.
- Group order. Order of an element.
- Direct product of groups.
- Group homomorphisms.
- Subgroups. Generating set. Finitely generated group.
- Cosets.
- Lagrange theorem.
- Primitive roots modulo n.
- Primitive roots modulo n: testing.
- Primitive roots modulo n: generating.

Binary functions

Let X be a set. A function $f : X \times X \to X$ is called a **binary function** on X. If there is no ambiguity (f is the only binary function) instead of writing $f(a, b)$ we write $a \cdot b$ or simply ab.

Definition

A binary function $\cdot$ is

- **commutative** if $ab = ba$ for every $a, b \in X$;
- **associative** if $(ab)c = a(bc)$ for every $a, b, c \in X$;
- **closed on a subset** $S \subset X$ if $ab \in S$ for every $a, b \in S$; in this event we also say that S is **closed under** $\cdot$. A restriction of $\cdot$ of $S \times S$ is a binary operation too.

We say that a and b **commute** in G if $ab = ba$.

Definition

An **algebraic structure** is a set X, perhaps, equipped with (unary, binary) functions and relations on X satisfying some conditions.

Groups

A group is one of the fundamental algebraic structures.

Definition

Let G be a set and $\cdot$ a binary operation on G. The pair $(G, \cdot)$ is called a **group** if:

(G1) There exists $e \in G$ (called the **identity element** of G) such that $eg = ge = g$ for every $g \in G$.
We often use the symbol 1 instead of e in the sequel.

(G2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every $a, b, c \in G$.

(G3) For every $a \in G$ there exists $b \in G$ (called the **inverse** of a and denoted by a^{-1}) such that $ab = ba = e$.

The group operation is often called a **law of composition**, or simply **multiplication**.

Definition

A group $(G, \cdot)$ is **abelian** if $\cdot$ is commutative.

Other examples of algebraic structures: fields, vector spaces, rings, monoids.

Groups: additive/multiplicative notation

For an abelian group we often (not always) use additive notation, i.e., we use operation $+$ and write $(G,+)$. That slightly changes our notation, the axioms (G1), (G2), (G3) become

(G1) $\exists e$ such that $e+g=g+e=g$.
It is natural to use the symbol 0 instead of e for the operation $+$.

(G2) $(a+b)+c=a+(b+c)$ for every $a,b,c\in G$.

(G3) $\forall a\ \exists b$ such that $a+b=b+a=0$.
It is natural to denote b as $-a$ in this case.

	$(G,\cdot)$	$(G,+)$
operation	$\cdot$	$+$
identity	1	0
inverse of a	a^{-1}	$-a$
power of a	a^n	na

Multiplicative vs additive group notation.

Groups: examples

- $(\mathbb{Z}, +)$ is an abelian group with identity 0. The inverse of $n \in \mathbb{Z}$ is $-n$.
- $(\mathbb{N}, +)$ is not a group.
- Similarly $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are groups.
- $(\mathbb{Z}, \cdot)$ is not a group, only 2 elements have inverses 1 and -1.
- The set $\{1, -1\} \subset \mathbb{Z}$ is a group under the usual multiplication.
- $(\mathbb{Q}, \cdot)$ is not a group, no inverse for 0.
- $(\mathbb{Q} - \{0\}, \cdot)$ is a group with identity 1 and inverses $(\frac{m}{n})^{-1} = \frac{n}{m}$ (here $m, n \neq 0$).
- Similarly $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$ are groups.
- $(\mathbb{Q}_+, \cdot)$ and $(\mathbb{R}_+, \cdot)$ are groups.
- The set of all bijections S_X on a set X is a group under composition.
- $(\mathbb{Z}_n, +)$ is an abelian group with the identity 0.
- Let p be a prime number. A fraction m/p^n is called a ***p*-adic fraction**. The set $\mathbb{Q}_p$ of all p-adic fractions is a group under addition.
- $(\mathbb{Z}_n, \cdot)$ is not a group.
- $(U_n, \cdot)$ is the **group of units**.

Order

Definition

- A group G is **finite** if it contains finitely many elements.
- The **order** $|G|$ of G is its cardinality (the number of elements it contains).
- The **order** $|g|$ of $g \in G$ is the least $n \in \mathbb{N}$ such that $g^n = e$, denoted by $|g|$.
- We say that G has **no torsion** (torsion-free) if every nontrivial element has infinite order. Otherwise, we say that G has torsion. $\square$

- $(\mathbb{Z}_n, +)$ is finite of order n. The order of 1 in $\mathbb{Z}_n$ is n.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are infinite. Every nontrivial element has infinite order.
- $(\mathbb{Q} - \{0\}, \cdot)$ is infinite. Every nontrivial element has infinite order.
- $(U_n, \cdot)$ is finite of order $\varphi(n)$.
- $|1| = 1$ in every multiplicative group.
- $|2| = 3$ in $\mathbb{Z}_3$, $|2| = 5$ in $\mathbb{Z}_5$, $|2| = 7$ in $\mathbb{Z}_7$, $|2| = 9$ in $\mathbb{Z}_9$, $|2| = 11$ in $\mathbb{Z}_{11}$.
- $|2| = 2$ in U_3, $|2| = 4$ in U_5, $|2| = 3$ in U_7, $|2| = 6$ in U_9, $|2| = 10$ in U_{11}.

Direct product of groups

Let $G_1, \ldots, G_n$ be groups. Consider the Cartesian product of $G_1, \ldots, G_n$

$$G = G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

and define a binary operation $\cdot$ on G as follows

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Proposition

The Cartesian product $G_1 \times \ldots \times G_n$ with binary operation $\cdot$ defined above is a group.

(G1) $(e_1, \ldots, e_n)$ is the identity,

(G2) operation is associative because for any $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n), c = (c_1, \ldots, c_n) \in G$ we have

$$(ab)c = ((a_1 b_1)c_1, \ldots, (a_n b_n)c_n) = (a_1(b_1 c_1), \ldots, a_n(b_n c_n)) = a(bc).$$

(G3) $(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$.

Proposition

$|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Direct product of groups: example

Consider the direct product $G = (U_5, \cdot) \times (\mathbb{Z}_5, +)$.

- $U_5 = \{1, 2, 3, 4\}$ and $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Hence, G is a set of pairs

  $$\begin{array}{ccccc} (1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\ (3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\ (4,0) & (4,1) & (4,2) & (4,3) & (4,4) \end{array}$$

  and its order is 20.
- $(1, 0)$ is the identity in G.
- $(3, 3) \cdot (3, 3) = (3 \cdot 3, 3 + 3) = (4, 1)$.
- $(3, 3)^{-1} = (2, 2)$.
- $(4, 4)^{-1} = (4, 1)$.
- $|(1, 1)| = 5$.
- $|(2, 1)| = 20$.

Homomorphism

Let G_1, G_2 be groups.

A map $\varphi : G_1 \to G_2$ is called a **homomorphism** *if $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in G_1$ (in which case we say that φ preserves multiplication).*

Warning! The identity $\varphi(ab) = \varphi(a)\varphi(b)$ depends on the operations in G_1 and G_2.

- ab is computed using the operation on G_1;
- $\varphi(a)\varphi(b)$ is computed using the operation on G_2.

- *$\varphi : (G_1, +) \to (G_2, \cdot)$ is a homomorphism if $\varphi(a + b) = \varphi(a) \cdot \varphi(b)$.*
- *$\varphi : (G_1, \cdot) \to (G_2, +)$ is a homomorphism if $\varphi(a \cdot b) = \varphi(a) + \varphi(b)$.*
- *$\varphi : (G_1, +) \to (G_2, +)$ is a homomorphism if $\varphi(a + b) = \varphi(a) + \varphi(b)$.*

Examples of homomorphisms

- For any groups G_1, G_2 the map $\varphi : G_1 \to G_2$ given by $\varphi(g) = e_2$ is the **trivial homomorphism**.
- Let $n \in \mathbb{N}$. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(m) = [m]_n$ is a homomorphism.
- Maps $\pi_1 : G_1 \times G_2 \to G_1$ and $\pi_2 : G_1 \times G_2 \to G_2$ defined by

$$(g_1, g_2) \overset{\pi_1}{\mapsto} g_1 \quad \text{and} \quad (g_1, g_2) \overset{\pi_2}{\mapsto} g_2$$

are group homomorphisms called **projection homomorphisms**.

Homomorphism

An injective homomorphism $\varphi : G_1 \to G_2$ is called a **monomorphism**.

A surjective homomorphism $\varphi : G_1 \to G_2$ is called an **epimorphism**.

A bijective homomorphism $\varphi : G_1 \to G_2$ is called an **isomorphism**. *We say that G_1 and G_2 are* **isomorphic** *and write $G_1 \simeq G_2$ if there is an isomorphism $G_1 \to G_2$.*

Main goal of group theory: *describe all groups up to isomorphism.*

Subgroups

A subset $H \subseteq G$ is a **subgroup** *of G and write $H \leq G$ if the following holds:*

(S1) *H is closed under $\cdot$;*

(S2) *$(H, \cdot)$ is a group itself.*

A subgroup $H \leq G$ is **proper** *if $H \neq G$.*

- $\{1\} \leq G$ (the **trivial subgroup**);
- $G \leq G$ (the **improper subgroup**);
- $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
- $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

*For $X \subseteq G$ define a set $\langle X \rangle = \{x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n} \mid x_i \in X$ **and** $\varepsilon_i = \pm 1\}$.*
Similarly, for $a \in G$ define a set $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proposition

Let $(G, \cdot)$ be a group, $X \subseteq G$, and $a \in G$. Then

- *$\langle X \rangle$ is the minimal subgroup of G containing X.*
- *$\langle a \rangle$ is the minimal subgroup of G containing a.*

Finitely generated subgroups of G

- *We say that $X \subseteq G$ is a* **generating set** *for G if $G = \langle X \rangle$.*
- *The subgroup $\langle a \rangle$ is called the* **subgroup generated by** *a.*
- *If $G = \langle X \rangle$, then we say that X* **generates** *G, or X is a* **generating set** *for G.*
- *G is* **cyclic** *if $G = \langle a \rangle$ for some $a \in G$.*
- *G is* **finitely generated** *if there exists a finite $X \subseteq G$ such that $G = \langle X \rangle$.*

Examples of generating sets:

- $(\mathbb{Z}, +) = \langle 1 \rangle$
- $(\mathbb{Z}_n, +) = \langle 1 \rangle$ is cyclic
- $U_5 = \langle 2 \rangle$ is cyclic
- $U_7 = \langle 3 \rangle$ is cyclic
- U_8 is not cyclic
- $U_9 = \langle 2 \rangle$ is cyclic
- $(\mathbb{Q}, +) = \langle 1/p^e \mid p$ is prime and $e \in \mathbb{N} \rangle$
- $(\mathbb{Z}^2, +) = \langle (1,0), (0,1) \rangle$ is not cyclic.
- $\{1, -1, i, -i\} = \langle i \rangle$
-
-
-

(Classification of cyclic groups)

If G is cyclic, then $G \simeq \mathbb{Z}_n$ or $G \simeq \mathbb{Z}$.

Cosets

- *The set $aH = \{ah \mid h \in H\}$ is called a **left coset** of $H \le G$.*
- *The set $Ha = \{ha \mid h \in H\}$ is called a **right coset** of $H \le G$.*

- $[a]_n = a + \langle n \rangle$ is a coset in $\mathbb{Z}$.
- $\langle 4 \rangle$ and $2\langle 4 \rangle$ are cosets in U_5.

If $a \in bH$, then $aH = bH$.

$$\begin{aligned} a \in bH \;\; &\Rightarrow \;\; a = bh^* \text{ for some } h^* \in H \\ &\Rightarrow \;\; ah = b(h^* h) \;\; \forall h \in H \;\; \Rightarrow \;\; aH \subseteq bH \\ &\Rightarrow \;\; b = a(h^*)^{-1} \text{ for some the same } h^* \\ &\Rightarrow \;\; bh = a\Big((h^*)^{-1} h\Big) \;\; \forall h \in H \;\; \Rightarrow \;\; bH \subseteq aH. \end{aligned}$$

For any $a, b \in G$ either $aH = bH$ or $aH \cap bH = \emptyset$.

The set of all left (resp. right) cosets forms a partition of G.

Lagrange theorem

$|aH| = |bH|$ for any $a, b \in G$, because $ah \mapsto bh$ is a bijection.

Theorem (Lagrange theorem for a finite group G)

- *If $H \leq G$, then $|H|$ divides $|G|$.*
- *If $a \in G$, then $|a|$ divides $|G|$.*

Because $|G| = \sum |aH| = |H| \cdot \#$ number of cosets.

The Lagrange theorem implies Fermat little theorem.

$$\begin{aligned} k = |a| = |\langle a \rangle| \text{ divides } |U_n| = \varphi(n) \quad &\Rightarrow \quad \varphi(n) = q \cdot |a| \\ &\Rightarrow \quad a^{\varphi(n)} = a^{q|a|} = \left(a^{|a|}\right)^q = 1. \end{aligned}$$

If $\gcd(a, n) = 1$, then $|a|$ is the least divisor d of $\varphi(n)$ satisfying $a^d \equiv_n 1$.

For instance, for $n = 53$ we have $\varphi(n) = 52 = 2^2 \cdot 13$. Hence, the order of any $a \in U_{53}$ is a positive divisor $1, 2, 4, 13, 26, 52$ of 52. For $a = 2$ we get

$$a^2 \equiv_{53} 4 \neq 1 \qquad a^{13} \equiv_{53} 30 \neq 1$$
$$a^4 \equiv_{53} 16 \neq 1 \qquad a^{26} \equiv_{53} 52 \neq 1,$$

and conclude that $|2| = 52$ in U_{53}.

Primitive roots modulo n

Definition

We say that $a \in \mathbb{Z}$ is a **primitive root modulo n** if $U_n = \langle a \rangle$.

- 2 is a primitive root modulo 3
- 3 is a primitive root modulo 4
- $2, 3$ are primitive roots modulo 5
- $3, 5$ are primitive roots modulo 7
- $2, 5$ are primitive roots modulo 9
- $2, 6, 7, 8$ are primitive roots modulo 11
- $2, 6, 7, 11$ are primitive roots modulo 13
- there are no primitive roots modulo 12.

Theorem

$$\begin{aligned} U_n \textit{ is cyclic} \quad &\Leftrightarrow \quad \textit{there are primitive roots modulo } n \\ &\Leftrightarrow \quad n = 2 \textit{ or } n = 4 \textit{ or } n = p^r \textit{ or } n = 2p^r, \textit{ where } p \textit{ is an odd prime} \end{aligned}$$

No proof.

Theorem

If there exists a primitive root modulo n, then there are $\varphi(\varphi(n))$ of them.

- U_n is cyclic $\quad \Leftrightarrow \quad U_n \simeq \mathbb{Z}_{\varphi(n)}$
- $\mathbb{Z}_{\varphi(n)} = \langle r \rangle \quad \Leftrightarrow \quad \gcd(\varphi(n), r) = 1$ for any $0 \le r < \varphi(n)$.
- The number of r's that are coprime with $\varphi(n)$ is $\varphi(\varphi(n))$.

Testing if a is a primitive root modulo n

Suppose that a is a unit modulo n.

$$\begin{aligned} a \text{ is a primitive root} \quad &\Leftrightarrow \quad |a| = \varphi(n) \text{ in } U_n \\ &\Leftrightarrow \quad \varphi(n) \text{ is the least positive number satisfying } a^{\varphi(n)} \equiv_n 1 \\ &\Leftrightarrow \quad a^d \not\equiv_n 1 \text{ for every divisor } d \text{ of } \varphi(n) \text{ less than } \varphi(n). \end{aligned}$$

(1) To check if $a = 3$ is a primitive root of $n = 53$ we compute

- $\varphi(n) = 52$.
- The divisors of 52 are $1, 2, 4, 13, 26, 52$. Compute the corresponding powers of 3

$$3^1 = 3, \quad 3^2 = 9, \quad 3^4 \equiv_{53} 28, \quad 3^{13} \equiv_{53} 30, \quad 3^{26} \equiv_{53} -1.$$

- Hence, $|3|_{53} = 52$ and 3 is a primitive root of 53.

(2) To check if $a = 5$ is a primitive root of $n = 41$ we compute

- $\varphi(n) = 40$.
- The divisors of 40 are $1, 2, 4, 5, 8, 10, 20, 40$. Compute the corresponding powers of 5

$$\begin{array}{llll} 5^1 = 5 & 5^2 = 9 & 5^4 \equiv_{41} 10 & 5^5 \equiv_{41} 9 \\ 5^8 \equiv_{41} 18 & 5^{10} \equiv_{41} 40 & 5^{20} \equiv_{41} 1. & \end{array}$$

- Hence, $|5|_{41} = 20$ and 5 is not a primitive root of 41.

Warning! *$\varphi(n)$ can have many divisors! Below we show that we do not need to test all of them if we simply want to check if a is primitive or not.*

Testing if a is a primitive root modulo n: a better approach

If $d_1 \mid d_2 \mid \varphi(n)$, then

$$a^{d_1} \equiv_n 1 \quad \Rightarrow \quad a^{d_2} \equiv_n 1.$$

Hence, if d_1 witnesses non-primitivity of a, then d_2 witnesses non-primitivity of a.

Hence, it is sufficient to check the greatest divisors of $\varphi(n)$.

(To check if a is a primitive root modulo n)

- *Check if* $\gcd(a, n) = 1$ *(must be true).*
- *Compute* $\mathrm{PPF}(\varphi(n)) = p_1^{a_1} \dots p_k^{a_k}$.
- *Check if* $a^{\frac{\varphi(n)}{p_i}} \equiv_n 1$ *(each must be false).*

If all conditions are satisfied, then output YES.

For instance,

- For $n = 53$, it is sufficient to check that $a^4 \not\equiv_{53} 1$ and $a^{26} \not\equiv_{53} 1$.
- For $n = 41$, it is sufficient to check that $a^8 \not\equiv_{41} 1$ and $a^{20} \not\equiv_{41} 1$.
- For $n = 79$, it is sufficient to check that $a^6 \not\equiv_{79} 1$, $a^{26} \not\equiv_{79} 1$, $a^{39} \not\equiv_{79} 1$.

Generating a primitive root modulo n

There is no efficient deterministic procedure to find a primitive root modulo n! We use a **randomized algorithm** for this purpose.

- Generate a random $2 \leq a < n$.
- Using $\mathrm{PPF}(\varphi(n))$, test if a is a primitive root.

Q. What is the chance that a randomly generated a is primitive modulo n?

$U_n \simeq \mathbb{Z}_{\varphi(n)}$, where $\mathrm{PPF}(\varphi(n)) = p_1^{a_1} \dots p_k^{a_k}$. A uniform choice of $a \in U_n$ corresponds a uniform choice of some $a' \in \mathbb{Z}_{\varphi(n)}$ and

$$a \text{ is a primitive root modulo } n \quad \Leftrightarrow \quad \gcd(a', \varphi(n)) = 1 \quad \Leftrightarrow \quad \begin{cases} p_1 \nmid a' \\ \vdots \\ p_k \nmid a' \end{cases}$$

The chance of the latter is

$$\frac{p_1 - 1}{p_1} \frac{p_2 - 1}{p_2} \dots \frac{p_k - 1}{p_k} \geq \frac{1}{2} \cdot \frac{2}{3} \cdot \dots \cdot \frac{k}{k+1} = \frac{1}{k+1} \geq \frac{1}{\log_2(\varphi(n)) + 1} > \frac{1}{\log_2(n) + 1},$$

which is good. E.g., to find a primitive number modulo a 1000 bit long prime p, we need to generate 1000 random a on average.