MPI - Lecture 5

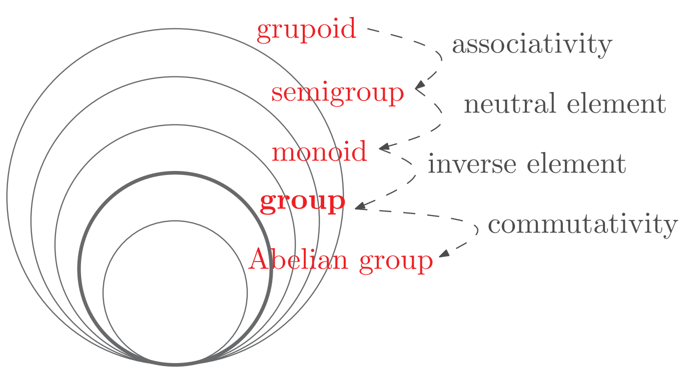
Outline

- Reminder and motivation
- Subgroups
- Groups generated by a set
- Cyclic groups

Reminder and Motivation

Reminder of the last lecture

Hierarchy of structures of type “a set and a binary operation”



Example (1/4)

Example 1. *Consider the set $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$ with the addition $\mod 12$.*

- *the set $\mathbb{Z}_{12}$ is closed under this operation, i.e., it is a **groupoid**groupoid;*
- *the operation is associative, so it is a **semigroup**semigroup;*
- *the number 0 is the neutral element, so it is a **monoid**monoid;*
- *the inverse of $k \neq 0$ is $12 - k$ and the inverse of 0 is 0, so it is a **group**group;*
- *the operation is commutative, thus we have an **Abelian group**.*

Let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ be the set of the residue classes modulo n.

The group $(\mathbb{Z}_n, +_{(\mathrm{mod}\ n)})$ is the additive group modulo n; it is denoted by $\mathbb{Z}_n^+$.

Question: Which other set M forms a group with the addition $(\mathrm{mod}\ 12)$?

In order for the operation to be well defined, we must have $M \subset \mathbb{Z}_{12}$:

Question (refined): Which subset of $\mathbb{Z}_{12}$ forms a group with the addition $(\mathrm{mod}\ 12)$?

Answer: There are quite a lot of them. To find out how to discover them, let us ask this subquestion:

Sub-question: Which is the smallest subset of $\mathbb{Z}_{12}$ that forms a group with addition $(\mathrm{mod}\ 12)$ and contains the number 2?

We are looking for a set $M \subset \mathbb{Z}_{12}$ such that $2 \in M$ and $(M, +_{(\mathrm{mod}\ 12)})$ is a group:

- M must be closed under addition $\mathrm{mod}\ 12$:
  - it must contain $2 + 2 = \mathbf{4}$, $2 + 4 = \mathbf{6}$, $4 + 6 = \mathbf{10}$, ...
  - the set $\{0, 2, 4, 6, 8, 10\}$ is closed under this operation, so we have a groupoid;

- the operation remains associative, so it is a semigroup;

- 0 remains the neutral element, so it is a monoid;

- each element has its inverse in the set (the set is closed under inversion), so it is a group.

The wanted set is $M = \{0, 2, 4, 6, 8, 10\}$.
We say that M is a subgroup generated by the set $\{2\}$.

Example (4/4)

Similarly, as we have generated the set from the element 2, we can proceed for others elements of $\mathbb{Z}_{12}$:

$$\begin{array}{rcl} \{0\} \rightarrow & \{0\} & \\ \{1\} \rightarrow & \{0,1,2,3,4,5,6,7,8,9,10,11\} & \leftarrow \{11\} \\ \{2\} \rightarrow & \{0,2,4,6,8,10\} & \leftarrow \{10\} \\ \{3\} \rightarrow & \{0,3,6,9\} & \leftarrow \{9\} \\ \{4\} \rightarrow & \{0,4,8\} & \leftarrow \{8\} \\ \{5\} \rightarrow & \{0,5,10,3,8,1,6,11,4,9,2,7\} & \leftarrow \{7\} \\ \{6\} \rightarrow & \{0,6\} & \end{array}$$

Back to the original question: there exist 6 different sets $M \subseteq \mathbb{Z}_{12}$ such that $(M, +_{(\text{mod } 12)})$ is a group.

Subgroups

Definition and basic properties

Definition of subgroup

Definition 2. *Let $G = (M, \circ)$ be a group.*

A subgroup of the group G is a pair $H = (N, \circ)$ such that:

- *$N \subseteq M$ and $N \neq \emptyset$,*
- *H is a group.*
- Idea of substructures with the same properties as the original structure: compare for instance with a subspace of a linear (vector) space.
- Similarly, we can define subgroupoids, subsemigroups, submonoids,...
- A binary operation in the group $G = (M, \circ)$ is a function from $M \times M$ to M.

  The operation in a subgroup $H = (N, \circ)$ is, to be precise, the restriction of this operation to the set $N \times N$.

Trivial and proper subgroups

In each group $G = (M, \circ)$, there always exist at least two subgroups (if M contains only one element the two coincide):

- the group containing only the neutral element: $(\{e\}, \circ)$, and
- the group itself $G = (M, \circ)$.

These two groups are the trivial subgroups.
Other subgroups are non-trivial or proper subgroups.

Question 3. *If H is a subgroup of a group G, is the neutral element of H identical to the neutral element of G?*

Intersection of subgroups

Theorem 4. *Let* $H_1, H_2, \ldots, H_n$*, whith* $n \geq 1$*, be subgroups of a group* $G = (M, \circ)$*. Then*

$$H' = \bigcap_{i=1,2,\ldots,n} H_i$$

is also a subgroup of G*.*

Power of an element

Definition 5. *Let* $G = (M, \circ)$ *be a group with neutral element* e*. We define for each element* $a \in M$ *and each positive* $n \in \mathbb{N}$ *the* n*-th power of the element* a *as*

$$\begin{aligned} a^0 &= e \\ a^n &= \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ times}} \\ a^{-n} &= (a^{-1})^n = \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n \text{ times}} \end{aligned}$$

Note that $a \circ a \circ \cdots \circ a$ can by written without brackets thanks to associativity (for a non-associative operation the result would depend on the order...).

For all $n, m \in \mathbb{N}$ the following "natural" equalities are true:

- $a^{n+m} = a^n \circ a^m$,
- $a^{nm} = (a^n)^m$.

For the additive notation of a group $G = (M, +)$, we define the n-th multiple of the element a and we denote it by $n \times a$ (resp. $-n \times a = n \times (-a)$).

Order of a subgroup

Order of a (sub)group

Definition 6. *The order of a (sub)group* $G = (M, \circ)$, *denoted* $|G|$, *is its number of elements. If* M *is an infinite set, the order is infinite.*

According to the order we distinguish between finite and infinite groups.

Example 7. *The group* $\mathbb{Z}_{12}^{+}$ *is of order* 12. *It has* 6 *subgroups:*

- *two trivial:* $\{0\}$ *and* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$;
- *and four proper:* $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, *and* $\{0, 2, 4, 6, 8, 10\}$.

of order 1, 2, 3, 4, 6 *and* 12.

(Left) cosets of a subgroup

Let G be a group and H be one of its subgroups.

The (left) coset of H in G with respect to an element $g \in G$ is the set

$$gH = \{gh : h \in H\} \quad \text{(or } g + H \text{ in additive notation)}$$

Example 8. *Let us consider the subgroup* $H = \{0, 3, 6, 9\}$ *of* $\mathbb{Z}_{12}$.

Find $g + H$ *for all* $g \in \mathbb{Z}_{12}$.

The index of H in G, denoted $[G : H]$, is the number of different cosets of H in G.

Lagrange's Theorem

Theorem 9. *Let* H *be a subgroup of a finite group* G. *The order of* H *divides the order of* G.

More precisely, $|G| = [G : H] \cdot |H|$.

This statement connects the abstract structure of a group with divisibility and also with the notion of prime numbers!

Consequence: A group with prime order has only trivial subgroups!

To prove Lagrange's Theorem we need the following lemma.

Lemma 10. *For all* $a, b \in G$ *one has* $|aH| = |bH|$.

Question 11. *Let* G *be a group of order* n *and* $k \in \mathbb{N}$ *be such that* $k|n$.

Is there any subgroup of G *of order* k?

Groups generated by a set

Group generated by a set (1/2)

Question: How to find the smallest subgroup of a group $G = (M, \circ)$ containing a given nonempty set $N \subset M$?

Definition 12. *Let $G = (M, \circ)$ be a group and $N \subset M$ a nonempty set. The smallest subgroup of G containing N is the subgroup generated by N and is denoted by $\langle N \rangle$.*

In particular, for a singleton $N = \{a\}$ we use the notation $\langle a \rangle = \langle \{a\} \rangle$.

Example 13. *For the group $\mathbb{Z}_{12}^{+}$, we have proven that $\langle 2 \rangle = (\{0, 2, 4, 6, 8, 10\}, +_{mod\ 12})$.*

Definition 14. *If for a set M it holds that $\langle M \rangle = G$, we say that M is a generating set of G.*

Group generated by a set (2/2)

Example 15. *The group $\mathbb{Z}_{12}^{+}$ is generated, for instance, by the sets $\{1\}$ and $\{5\}$, i.e.*

$$\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_{12}^{+}.$$

Theorem 16. *Let $G = (M, \circ)$ be a group and $N \subset M$ a nonempty set. The following holds:*

- *the subgroup $\langle N \rangle$ equals the intersection of all subgroups containing N, i.e.*

$$\langle N \rangle = \bigcap \{H : H \text{ is a subgroup of } G \text{ containing } N\}$$

- *all elements in $\langle N \rangle$ can be obtained by means of "group span", i.e.,*

$$\left\{ a_1^{k_1} \circ a_2^{k_2} \circ \cdots a_n^{k_n} \ : \ n \in \mathbb{N},\ a_i \in N,\ k_i \in \mathbb{Z} \right\}.$$

Cyclic groups

Examples

Groups generated by one element (1/2)

We have seen that the additive group $\mathbb{Z}_{12}^{+}$ is equal to $\langle 1\rangle$, $\langle 5\rangle$, $\langle 7\rangle$, and $\langle 11\rangle$.

The following theorem generalize this fact.

Theorem 17. *An additive group modulo n is equal to $\langle k\rangle$ if and only if k and n are coprimes.*

Proof. This statement is a consequence of a general theorem which will be proven later and of the fact that $\mathbb{Z}_n^{+} = \langle 1\rangle$ for all $n \geq 2$. □

Groups generated by one element (2/2)

The group $(\{1, 2, \ldots, p-1\}, \cdot_{(\text{mod } p)})$, where p is a prime number, is the multiplicative group modulo p, denoted $\mathbb{Z}_p^{\times}$.

Example 18. *Is there a one-element set generating the group $\mathbb{Z}_{11}^{\times}$?*

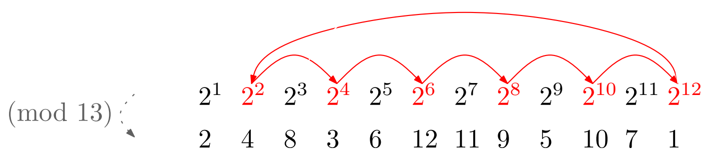
Yes, for example $\langle 2\rangle = \mathbb{Z}_{11}^{\times}$.

On the other hand, $\langle 3\rangle = (\{1, 3, 4, 5, 9\}, \cdot_{(mod\ 11)})$.

Finding the generator(s) of a multiplicative group $\mathbb{Z}_p^{\times}$ is more complicated than for an additive group $\mathbb{Z}_n^{+}$.

Multiplicative groups have more complicated and interesting structure.

(mod 13)	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
	2	4	8	3	6	12	11	9	5	10	7	1



Definition

Definition of cyclic group

Definition 19. *A group $G = (M, \circ)$ is cyclic if there exists an element $a \in M$ such that $\langle a \rangle = G$.*

This element is a generator of the cyclic group.

- $\mathbb{Z}_n^+$ is a cyclic group for every n and its generators are all positive numbers $k \leq n$ coprime with n.

- The infinite group $(\mathbb{Z}, +)$ is cyclic and it has just two generators: 1 and -1.

- $\mathbb{Z}_{11}^\times$ is cyclic, and 2 is a generator.

Why “cyclic”?

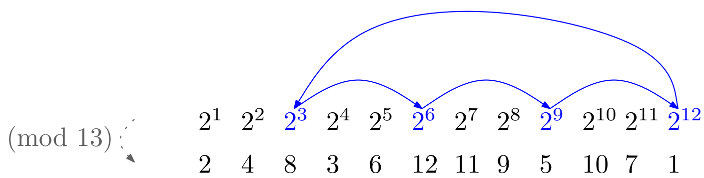
Consider the multiplicative group $\mathbb{Z}_{13}^\times$.

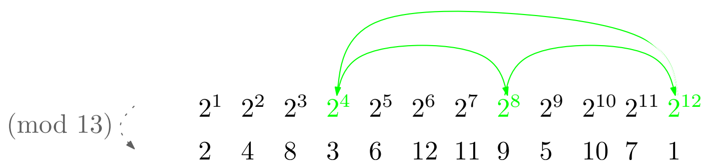
If we repeatedly compose the generator 2 with itself we successively get all elements of the group: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 3$, $\ldots$, $2^{12} = 1$.

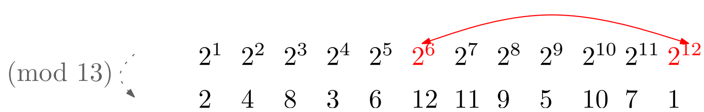
The 13-th power is again the number 2 and so the sequence of powers is indeed stuck in a cycle.

subgroups: $\{1, 3, 4, 9, 10, 12\}$,$\{1, 5, 8, 12\}$,$\{1, 3, 9\}$,$\{1, 12\}$.

generators: 2, 6, 7, 11.







Fermat's Theorem

Fermat's Theorem (1/2)

Theorem 20. *In a cyclic group $G = (M, \circ)$ of order n, for all elements $a \in M$, it holds that*

$$a^n = e$$

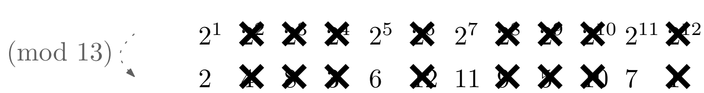
Where e is the neutral element of G.

Proof. Consider a sequence of elements from M: $a, a^2, a^3, a^4, \ldots$

Denote q the smallest number such that $a^q = e$. Clearly $q \leq n$ (why?!)

The set $a, a^2, \cdots, a^q$ is the subgroup $\langle a \rangle$ and has order q.

By Lagrange's Theorem, we have that q divides n, i.e,. there exists $k \in \mathbb{N}$ such that $n = qk$.



We have $a^n = a^{qk} = (a^q)^k = e^k = e$. □

Fermat's Theorem (2/2)

$\mathbb{Z}_p^\times$ is always a cyclic group (it is not trivial to prove it) and its order is $p-1$.

Applying the previous theorem to $\mathbb{Z}_p^\times$ we obtain the well-known Fermat's Little Theorem.

Corollary 21 (Fermat's Little Theorem)**.** *For an arbitrary prime number p and an arbitrary $1 \leq a < p$ we have that*

$$a^{p-1} \equiv 1 \, (mod \; p).$$

Find the generators

How to find all generators (1/2)

Generally, to find all generators is not an easy task (e.g., in groups $\mathbb{Z}_p^\times$ we are not able to do it algorithmically); but if we have one, it is easy to find all the others.

Theorem 22. *If $(G, \circ)$ is a cyclic group of order n and a is one of its generator, then a^k is a generator if and only if k and n are coprime.*

To prove the previous theorem we use the following

Lemma 23. *Let $D = \{mk + \ell n \mid m, \ell \in \mathbb{Z}\}$.*
Then $\gcd(k, n) = \min\{|a| \mid a \in D \setminus \{0\}\}$.

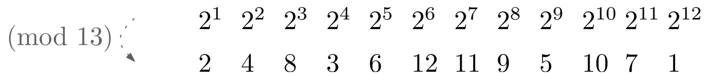
How to find all generators (2/2)

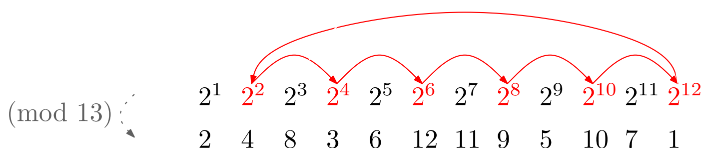
Corollary 24. *In a cyclic group of order n, the number of all generators is equal to $\varphi(n)$.*

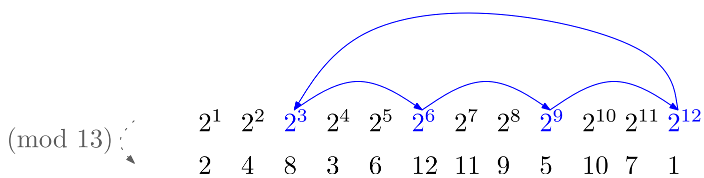
Where φ is the Euler's (totient) function, which assigns to each integer n the number of integers less than n that are coprime with n

$\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$ and thus it has $\varphi(p-1)$ generators.

An effective algorithm for evaluating $\varphi(n)$ does not exist; if it existed, we would be able to find the integer factorization of arbitrarily large n and RSA would not be safe!







Subgroups of cyclic groups

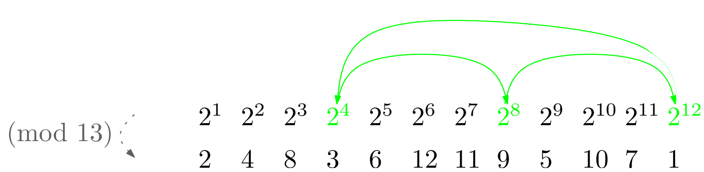
Subgroups of cyclic group are cyclic

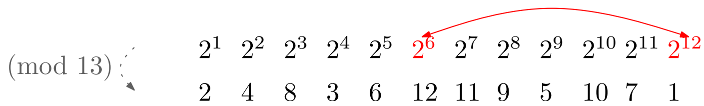
Theorem 25. *Any subgroup of a cyclic group is again a cyclic group.*

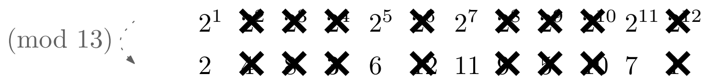
Consider again the multiplicative group $\mathbb{Z}_{13}^{\times}$.
subgroups: $\{1,3,4,9,10,12\}$, $\{1,5,8,12\}$, $\{1,3,9\}$, $\{1,12\}$.
generators: 2, 6, 7, 11.

Order of an element

Order of an element







Let G be a group and $g \in G$.

The order of g (in G) is the order of the group that is generated by g.

In the finite case, we have the equivalence $\text{order}(g) = \#\langle g \rangle$.

Example 26. *Find the order of all elements in* $\mathbb{Z}_5^\times$ *and in* $\mathbb{Z}_7^\times$.