Abelian groups

Mathematical Cryptography, Lectures 7 - 8

Contents

Groups and abelian groups

Definition

- A set G with a binary operation $*$ forms a *group*, in case the operation $*$ is associative, has an identity element, and every element has an inverse.
- Moreover, if a group operation is commutative, we speak about a commutative group or an *abelian group*.

Examples

- $(\mathbb{Z}_n, +)$ is an abelian group of order n (additive group)
- $(\mathbb{Z}_n, \cdot)$ is not a group, at least 0 has no inverse
- $(\mathbb{Z}_n^*, \cdot)$ is the abelian group of order $\varphi(n)$ (multiplicative group)

The number of elements of a group is called the *order of the group*.

Groups and abelian groups

Additive and multiplicative notation

- Additive notation: $(G, +, 0, -(\cdot))$
  the operation is $+$, the zero element 0, the opposite element to a is $-a$;
  iterated addition gives a multiple $\underbrace{a + a + \ldots + a}_{k\ times} = ka$
- Multiplicative notation: $(G, \cdot, 1, (\cdot)^{-1})$
  the operation $\cdot$, the identity element 1, the inverse of a is a^{-1};
  iterated multiplication gives a power $\underbrace{a \cdot a \cdot \ldots \cdot a}_{k\ times} = a^k$

Note: We will use multiplicative notation mostly.

Groups and abelian groups

Powers of elements

Let $(G, \cdot)$ be a group with the identity element 1, $a \in G$, $k \in \mathbb{Z}$. We define an integer power of the element a as follows:

- for $k > 0$ is $a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k\ times}$ (due to associativity)
- $a^0 = 1$ (due to the identity element)
- for $k < 0$, $a^k = (a^{-1})^{|k|}$ (due to the inverse of a)

Proposition

Well-known formulas hold: $a^{k+l} = a^k a^l$, $(a^k)^l = a^{kl}$
Moreover, in an abelian group: $(ab)^k = a^k b^k$

Groups and abelian groups

Proposition

Let $(G, \cdot)$ be a group.

- The identity element is uniquely determined.
  If e is the left identity element and f is the right identity element, then $e = f$ is the identity element.
- The inverse element of a is uniquely determined.
  If b is the left inverse of a, c the right inverse of a, then $b = c$ is the inverse of a.
- Socks and shoes lemma:
  In a (non-commutative) group, $(ab)^{-1} = b^{-1}a^{-1}$.

Groups and abelian groups

Proposition

Let $(G, \cdot)$ be a group.

- The cancellation law holds in the group G, i.e. for every $a \in G$: if $a \cdot x = a \cdot y$, then $x = y$.
  This property does not characterize groups: in $(\mathbb{Z}, \cdot)$ one can also cancel with any element, even though it is not a group.
- All linear equations $a \cdot x = b$, $y \cdot a = b$ have a solution in the group G, and this solution is unique.
  This property characterizes groups: every semigroup in which all linear equations have a solution already is a group.
- A left translation by an element of $a \in G$, the map $l_a : G \to G : x \mapsto a \cdot x$, is a bijection.

Rings and fields

Remark

- $(R, +, \cdot)$ is called *ring* in case $(R, +)$ is a commutative group, $(R, \cdot)$ is a semigroup, and both distributive laws hold.
  A nontrivial ring with unity is called a *domain* if the cancellation law holds for any nonzero element.
  A non-trivial ring is a *field* if $(R - \{0\}, \cdot)$ is a group.
- A non-trivial ring is a field if and only if all linear equations $a \cdot x = b$, $y \cdot a = b$, where $a \neq 0$, have a solution.
- Every finite domain is a field, because an injection l_a is a mapping from a finite set to itself, so it must be a bijection.

Groups and abelian groups

Definition

If $G_1, \ldots, G_k$ are groups, then the set $G_1 \times \ldots \times G_k$ of all $k-$tuples together with the operation defined component-wise (in the i'th component one counts as in G_i) is also a group. It is called the *direct product* of the groups $G_1, \ldots, G_k$.
If all groups are equal, $G_i = G$ for $1 \leq i \leq k$, we speak of the direct power of G and we denote it by $G^{\times k}$.

Remark

The direct product of groups was used in the Chinese remainder theorem. For example, $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$.

Subgroups

Definition

A subset H of the group $(G, \cdot, 1, (\cdot)^{-1})$ forms an subgroup if for every $a, b \in G$ the following holds:

- if $a, b \in H$, then $ab \in H$
- $1 \in H$
- if $a \in H$, then $a^{-1} \in H$

It means, a subgroup is a subset of the group, which is closed to the binary operation, to the identity element and all inverse elements.

Subgroups

Proposition

Let G be a group and $\emptyset \neq H \subseteq G$. The following statements are equivalent:

- H is a subgroup in G
- for all $a, b \in G$: if $a, b \in H$, then $ab \in H$ and $a^{-1} \in H$
- for all $a, b \in G$: if $a, b \in H$, then $ab^{-1} \in H$

Proposition

Let H_1, H_2 be subgroups in the group G.

- $H_1 \cap H_2$ is a subgroup in G.
- If, moreover, G is abelian, then $H_1 \cdot H_2 = \{h_1 h_2;\ h_1 \in H_1, h_2 \in H_2\}$ is a subgroup in G.

Subgroups

Examples

Let G be a group.

- Obviously $\{1\}$ and G are subgroups of the group G.
- The set of all integer powers of the element $a \in G$, $M = \{a^k, k \in \mathbb{Z}\}$ is a subgroup of G. We call it the *cyclic subgroup* generated by a, we denote it by $\langle a \rangle$.

In the additive group $(G, +)$, the cyclic group $\langle a \rangle$ is the set of all integer multiples of the element $a \in G$.

Subgroups in $\mathbb{Z}$ and in $\mathbb{Z}_n$

Proposition

Every subgroup in $(\mathbb{Z}, +)$ is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$.
Moreover: $m_1\mathbb{Z} \subseteq m_2\mathbb{Z}$ just when $m_2 \mid m_1$.

Proposition

Every subgroup in $(\mathbb{Z}_n, +)$ is of the form $d\mathbb{Z}_n$ for some $d \in \mathbb{Z}$, where $d \mid n$.
Moreover: $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$ just when $d_2 \mid d_1$.

Thus, every subgroup of $(\mathbb{Z}_n, +)$ is cyclic.
For each divisor d of n there is one subgroup of the form $d\mathbb{Z}_n$.
This subgroup has $\frac{n}{d}$ elements.

.

Cosets of a subgroup

Definition

Let G be a group, H a subgroup of G, $a \in G$.
The *left coset of the subgroup* H determined by an element a is the set $aH = \{ah, h \in H\}$.
The right coset Ha is defined analogously.

Remark

If G is an abelian group, then $aH = Ha$ (and we denote it as $[a]_H$) for every $a \in G$.
The number of different cosets of H in G is called the *index of the subgroup* H in the group G, and denoted $[G : H]$.

Cosets of a subgroup

Proposition

- For every $a \in G$, $|aH| = |H|$.
- All left cosets form a partition on the set G, i.e. $G = \bigcup_{a \in G} aH$, and aH, bH are either the same or disjunctive.

Lagrange's theorem

Let G be a finite group and H a subgroup of G.
The order of the subgroup H divides the order of the group G, more precisely $|G| = [G : H] \cdot |H|$.

Remark

For subsemigroups of a finite semigroup, something similar does not hold. For example, in the semigroup of left zeros, every subset forms a subsemigroup.

Quotient group modulo a subgroup

Proposition

Let G be an abelian group and H be a subgroup in G.

- The prescription $aH \cdot bH = abH$ correctly defines an operation on cosets. (Due to commutativity, the result does not depend on the choice of cosets representatives.)
- The set of all cosets of H in G together with this operation again forms a group. It is called the *quotient group* of G modulo H and is denoted by G/H.

Remark

The noncommutative group G can be factorized only modulo a *normal subgroup* H, for which $aH = Ha$ holds for all $a \in G$.

Congruence modulo a subgroup

Example

$(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$
Let us remind that $\mathbb{Z}_n$ was previously made through factoring by congruence modulo n, where $a \equiv b \pmod{n}$ in case $n \mid a - b$, or equivalently $a - b \in n\mathbb{Z}$.

Definition

Let G be an abelian group, H a subgroup in G, $a, b \in G$.
We say that a is *congruent* with b *modulo the subgroup* H, $a \equiv b \pmod{H}$ in case $ab^{-1} \in H$.

Claim

The following statements are equivalent.
$a \equiv b \pmod{H}$ iff $Ha = Hb$ iff $a = hb$ for some $h \in H$.

Congruence modulo a subgroup

Proposition

- The congruence modulo a subgroup is an equivalence relation on the set G, so it splits G into classes, and these classes are exactly the cosets aH, for $a \in G$. (This holds for all groups.)
- The congruence modulo a subgroup is preserved by the binary operation (this applies only to abelian groups), so we can define a binary operation on classes via representatives.
- This constructs a factor group of the group G by congruence modulo H, which is exactly the quotient group G/H.

For non-commutative groups, one can only introduce the congruence modulo a normal subgroup.

Quotient domain modulo an ideal

Remark

- Let $(R, +, \cdot)$ be a commutative ring. The subset $I \subset R$ is called the *ideal* of the ring R in case
  - $(I, +)$ is a subgroup of $(R, +)$,
  - for all $r \in R$ and all $i \in I$ holds $r \cdot i \in I$.
- If we want to create a *commutative quotien ring*, we must count modulo an ideal, so that addition and multiplication on cosets can be defined correctly via representatives.
- Each ideal in $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. The quotient ring modulo an ideal $m\mathbb{Z}$ is just $(\mathbb{Z}/m\mathbb{Z}, +, \cdot) = (\mathbb{Z}_m, +, \cdot)$ the factor ring of residue classes modulo m.

Group homomorphisms

Definition

Let $(G_1, \cdot)$ and $(G_2, \circ)$ be groups.
A map $f : G_1 \rightarrow G_2$ is called the *group homomorphism* in case for all $a, b \in G_1$ the following holds:

- $f(a \cdot b) = f(a) \circ f(b)$
- $f(1) = 1$
- $f(a^{-1}) = f(a)^{-1}$

Proposition

Let $(G_1, \cdot)$ and $(G_2, \circ)$ be groups.
A map $f : G_1 \rightarrow G_2$ is the group homomorphism, if and only if for all $a, b \in G_1$ holds $f(a \cdot b) = f(a) \circ f(b)$.

Group homomorphisms

Examples

- For any groups G_1 and G_2, the map $f : G_1 \to G_2 : a \mapsto 1$ is a group homomorphism.
- Let H be a subgroup of the group G.
  The embedding $i : H \to G : h \mapsto h$, and the natural projection $\pi : G \to G/H : a \mapsto aH$ are group homomorphisms.
- For any group G and for any $a \in G$, the integer exponentiation map $f : (Z, +) \to G : z \mapsto a^z$ is a group homomorphism.
- For any abelian group G, the $m-$th power map on G, $\rho : G \to G : a \mapsto a^m$ is a group homomorphism.

Group isomorphisms

Definition

Let $(G_1, \cdot)$ and $(G_2, \circ)$ be groups.
A group homomorphism $f : G_1 \to G_2$, which is a bijection too, is called the *group isomorphism*.

Proposition

Let $n = \prod_{i=1}^{k} p_i^{e_i}$, where the primes p_i are different.
The reminder map $\theta : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \ldots \ldots \times \mathbb{Z}_{p_k^{e_k}} : a \mapsto (a_1, \ldots, a_k)$, where $0 \leq a_i < p_i^{e_i}$ satisfy $a \equiv a_i \pmod{p_i^{e_i}}$, is a group isomorphism of additive groups: $\mathbb{Z}_n \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$

The restriction of θ to the set $\mathbb{Z}_n^*$ is a group isomorphism of multiplicative groups: $\mathbb{Z}_n^* \cong \mathbb{Z}^*_{p_1^{e_1}} \ldots \times \mathbb{Z}^*_{p_k^{e_k}}$

Ring homomorphisms

Remark

- Let $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ be commutative rings with unit.
  A map $f : R_1 \to R_2$ is called the *ring homomorphism*, in case it is a group homomorphism of additive groups and it respects multiplication and the identity element.
- A map f is a ring homomorphism iff for all $a, b \in R_1$,
  $f(a+b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$, $f(1) = 1$.
- The Chinese reminder map θ is a ring isomorphism.

Group isomorphisms

Proposition

Let G be an abelian group, H_1, H_2 its subgroups.
If $H_1 \cap H_2 = 1$, then $H_1 \times H_2 \cong H_1 \cdot H_2$, where the map
$f : H_1 \times H_2 \to H_1 \cdot H_2 : (h_1, h_2) \mapsto h_1 h_2$ is a group isomorphism.

Definition

Let G be an abelian group, H_1, H_2 its subgroups.
If $G = H_1 \cdot H_2$ and $H_1 \cap H_2 = 1$, then the group G is called the *internal direct product* of the subgroups H_1 and H_2.
We denote it by $G = H_1 \dot{\times} H_2$.

In this case, every element $g \in G$ can be written uniquely in the form $g = h_1 h_2$ for some $h_1 \in H_1$, $h_2 \in H_2$.

Group homomorphisms

Definition

Let $f : G_1 \to G_2$ be a group homomorphism.

- The *image* of f is the set $Im\, f = \{b \in G_2; b = f(a) \text{ for some } a \in G_1\}$.
- The *kernel* of f is the set $Ker\, f = \{a \in G_1; f(a) = 1\}$.

Proposition

Let $f : G_1 \to G_2$ be a group homomorphism.

- $Ker\, f$ is a subgroup of the group G_1 (even a normal subgroup).
- $Im\, f$ is a subgroup of the group G_2.
- The image of a subgroup is a subgroup too and the preimage of a subgroup is a subgroup too.
- f is injective, if and only if $Ker\, f = \{1\}$.

Group homomorphisms

The first isomorphism theorem

Let $f : G \to G'$ be a group homomorphism.
Then $G/Ker\, f \cong Im\, f$.
Specially, the map $\varphi : G/Ker\, f \to G' : a\, Ker\, f \mapsto f(a)$
is an injecvite group homomorphism whose image is $Im\, f$.

So it holds, that $\varphi \circ \pi = f$ where π is the natural projection and the operation $\circ$ is the composition of mappings.

Remark

Let $f : R \to R'$ be a ring homomorphism, then $R/Ker\, f \cong Im\, f$.
Here, the quotient ring $R/Ker\, f$ can be constructed because $Ker\, f$ always is an ideal in R.

Group homomorphisms

Consequence

Let $f : G \to G'$ be a group (a ring) homomorphism.
Then each element $b \in Im\, f$ has the same number of preimages.

If the element a is one of preimages of b, then the equation $f(x) = b$ is solved by all elements of the coset $a\, Ker\, f$.

Each solution has a form $x = ac$, where $c \in Ker\, f$ solves the equation $f(x) = 1$.

This fact (in its additive form) is well known from solving systems of linear equations.

Group homomorphisms

m−th powers and roots

Let G be an abelian group, then the power map $\rho : G \to G : a \mapsto a^m$ is a group homomorphism.

- $Ker\,\rho = \{a \in G, a^m = 1\} = {}_G\sqrt[m]{1}$ (the set of all m-th roots of 1) is a subgroup of G.
- $Im\,\rho = \{a^m, a \in G\} = G^m$ (the set of all m-th powers of elements of G) is a subgroup of G.
- $G/Ker\,\rho \simeq Im\,\rho$, where the corresponding isomorphism is $\varphi : aKer\rho \mapsto a^m$.

Each element of $b \in G^m$ has the same number of $m-$th roots. If we find one solution to the equation $x^m = b$, let's denote it by a, then every solution has a form $x = ac$, where c solves $x^m = 1$.

Abelian groups

Literature

- Shoup: A Computational Introduction to Number Theory and Algebra. Chapter 6.1-4.
  http://shoup.net/ntb/
- Considering rings, see Chapter 7.