

AFCS / Spring 2015

## *Groups*

Prof.Dr. Ferucio Laurențiu Țiplea

“Al. I. Cuza” University of Iași  
Department of Computer Science  
Iasi 740083, Romania

E-mail: [ftiplea@mail.dntis.ro](mailto:ftiplea@mail.dntis.ro)

URL: <http://www.infoiasi.ro/~ftiplea>

# Contents

---

1. Definitions, examples, basic properties
2. Subgroups. Lagrange's theorem
3. Cyclic groups
4. The group  $\mathbb{Z}_m^*$
5. The discrete logarithm problem
6. Applications to cryptography

# 1. Definitions, examples, basic properties

**Definition 1** A **group** is a 4-tuple  $(G, \cdot, ', e)$  which consists of a set  $G$ , a binary operation  $\cdot$  on  $G$ , a unary operation  $'$  on  $G$ , and a nullary operation  $e \in G$  such that:

- $\cdot$  is associative;
- $(\forall x \in G)(x \cdot e = e \cdot x = x)$ ;
- $(\forall x \in G)(x \cdot x' = x' \cdot x = e)$ .

**Remark 1** Let  $(G, \cdot, ', e)$  be a group.

1. The element  $e$  is called the **unity** of  $G$ . It is **unique** and it is also denoted by  $1_G$  or even  $1$ ;
2. For any  $x$ ,  $x'$  is **unique** with the property  $x \cdot x' = x' \cdot x = e$ .  $x'$  is called the **inverse** of  $x$  and it is also denoted by  $x^{-1}$ .

# 1. Definitions, examples, basic properties

Conventions to be used when no confusions may arise:

- We will usually denote groups just by their carrier sets. That is, we will often say “Let  $G$  be a group”;
- When the binary operation of a group is denoted additively (by  $+$ ), then the unary operation will be denoted by “ $-$ ” and the nullary operation by  $0$ . However, in such a case, “ $-$ ” should not be confused with the subtraction operation, and  $0$  with the number zero.
- We will often omit the symbol of the binary operation when two or more elements of the group are operated by it. That is, we will write  $ab$  instead of  $a \cdot b$ .

**Definition 2** A group  $(G, \cdot, ', e)$  is called **commutative** if  $\cdot$  is a commutative operation.

# 1. Definitions, examples, basic properties

## Basic notations:

### 1. multiplicatively denoted groups:

- $a^0 = e$ ;
- $a^n = a^{n-1} \cdot a$ , for any  $n \geq 1$ ;
- $a^{-1} = a'$ , where  $a'$  is the inverse of  $a$ ;
- $a^{-n} = (a^{-1})^n$ , for any  $n \geq 1$ ;

### 2. additively denoted groups:

- $0a = 0$ ;
- $na = (n-1)a + a$ , for any  $n \geq 1$ ;
- $(-1)a = -a$ , where  $-a$  is the inverse of  $a$ ;
- $(-n)a = n(-a)$ , for any  $n \geq 1$ ,

# 1. Definitions, examples, basic properties

**Proposition 1** Let  $G$  be a group,  $a, b \in G$ , and  $m, n \in \mathbb{Z}$ . Then, the following properties hold true:

- (1)  $(a^{-1})^{-1} = a$ ;
- (2)  $(ab)^{-1} = b^{-1}a^{-1}$ ;
- (3)  $a^m a^n = a^{m+n} = a^n a^m$ ;
- (4)  $(a^m)^n = a^{mn} = (a^n)^m$ ;
- (5)  $a^{-m} = (a^{-1})^m = (a^m)^{-1}$ .

You are invited to rewrite these properties under the additive notation.

# 1. Definitions, examples, basic properties

## Example 1

1.  $(\mathbb{Z}, +, -, 0)$ ,  $(\mathbb{Q}, +, -, 0)$ ,  $(\mathbb{R}, +, -, 0)$ , and  $(\mathbb{C}, +, -, 0)$  are commutative groups.
2.  $(\mathbb{Q}^*, \cdot, ^{-1}, 1)$ ,  $(\mathbb{R}^*, \cdot, ^{-1}, 1)$ , and  $(\mathbb{C}^*, \cdot, ^{-1}, 1)$  are commutative groups.
3.  $(n\mathbb{Z}, +, -, 0)$  is a commutative group, and  $(n\mathbb{Z}, \cdot, 1)$  is a commutative monoid.
4.  $(\mathbb{Z}_m, +, -, 0)$  is a **cyclic** commutative group, and  $(\mathbb{Z}_m^*, \cdot, ^{-1}, 1)$  is a commutative group, for any  $m \geq 1$ .
5. Let  $A$  be a set. The set of all bijective function from  $A$  to  $A$ , together with the function composition operation, the function inverse operation, and the identity function from  $A$  to  $A$ , forms a groups called the **permutations group of  $A$**  or the **symmetric group of  $A$** . It is usually denoted by  $Sym(A)$ .

# 1. Definitions, examples, basic properties

---

## Solving equations in groups:

**Proposition 2** Let  $G$  be a semigroup.

- (1) If  $G$  is a group, then, for any  $a, b \in G$ , the equations  $ax = b$  and  $ya = b$  have unique solutions in  $G$ .
- (2) If, for any  $a, b \in G$ , the equations  $ax = b$  and  $ya = b$  have unique solutions in  $G$ , then  $G$  is a group.



## 2. Subgroups. Lagrange's theorem

**Definition 3** A group  $(H, \circ, '' , e_H)$  is a **subgroup** of a group  $(G, \cdot, ' , e_G)$  if  $\circ = \cdot|_H$ ,  $'' = ' |_H$ , and  $e_H = e_G$ .

When  $H$  is a subgroup of  $G$  we will write  $H \leq G$ .

**Example 2** Considering the groups in Example 1, it follows:

- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ ;
- $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ ;
- $n\mathbb{Z} \leq \mathbb{Z}$ , for any  $n \in \mathbb{Z}$ . Moreover, any subgroup of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ , for some  $n \geq 0$ .

## 2. Subgroups. Lagrange's theorem

**Proposition 3** Let  $(G, \cdot, ', e)$  be a group and  $H \subseteq G$  a non-empty subset. The following statements are equivalent:

- (1)  $H \leq G$ ;
- (2)  $ab \in H$  and  $a' \in H$ , for any  $a, b \in H$ ;
- (3)  $ab' \in H$ , for any  $a, b \in H$ .

**Corollary 1** Let  $(G, \cdot, ', e)$  be a finite group. Then, a non-empty subset  $H$  of  $G$  is a subgroup of  $G$  iff  $ab \in H$ , for any  $a, b \in H$ .

## 2. Subgroups. Lagrange's theorem

Let  $G$  be a group and  $H \leq G$ . Define two binary relations on  $G$ ,  $\sim_H$  and  ${}_H\sim$ , by

$$\bullet \quad a \sim_H b \iff (\exists c \in H)(b = ac)$$

$$\bullet \quad a {}_H\sim b \iff (\exists c \in H)(b = ca),$$

for  $a, b \in G$ .

**Proposition 4** Let  $G$  be a group,  $H \leq G$ , and  $a, b \in G$ .

$$\bullet \quad a \sim_H b \text{ iff } a'b \in H.$$

$$\bullet \quad a {}_H\sim b \text{ iff } ba' \in H.$$

$$\bullet \quad \sim_H \text{ and } {}_H\sim \text{ are equivalence relations on } G.$$

$$\bullet \quad [a]_{\sim_H} = aH \text{ and } [a]_{{}_H\sim} = Ha.$$

$$\bullet \quad H, aH, \text{ and } Ha \text{ are pairwise equipotent sets.}$$

$$\bullet \quad \{Ha | a \in G\} \text{ and } \{aH | a \in G\} \text{ are equipotent sets.}$$

## 2. Subgroups. Lagrange's theorem

---

Let  $G$  be a finite group and  $H \leq G$ . The **index of  $H$  in  $G$**  is defined by

$$(G : H) = |\{Ha | a \in G\}| = |\{aH | a \in G\}|.$$

**Theorem 1** (Lagrange's Theorem)

For any finite group  $G$  and  $H \leq G$ ,

$$|G| = (G : H)|H|.$$

### 3. Cyclic groups

A group  $G$  is **cyclic** if it can be generated by one of its elements. That is,

- if  $G$  is written multiplicatively, then  $G$  is cyclic if

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\},$$

for some  $a \in G$ ;

- if  $G$  is written additively, then  $G$  is cyclic if

$$G = \langle a \rangle = \{na \mid n \in \mathbb{Z}\},$$

for some  $a \in G$ .

### 3. Cyclic groups

---

#### Example 3

1.  $(\mathbb{Z}, +, -, 0)$  is an infinite cyclic group generated by 1.
2. For any  $m \geq 1$ ,  $(\mathbb{Z}_m, +, -, 0)$  is a finite cyclic group:
  - if  $m = 1$ , then the group is generated by 0;
  - if  $m > 1$ , then the group is generated by 1.

### 3. Cyclic groups

**Theorem 2** Let  $a$  be an element of a group  $(G, \cdot, ', e)$ . Then, exactly one of the following two properties holds true:

- (1)  $a^n \neq a^m$  for any integers  $n \neq m$ , and the cyclic subgroup generated by  $a$  is isomorphic to  $(\mathbb{Z}, +, -, 0)$ ;
- (2) there exists  $r > 0$  such that:
  - (a)  $a^r = e$ ;
  - (b)  $a^u = a^v$  iff  $u \equiv v \pmod{r}$ , for any  $u, v \in \mathbb{Z}$ ;
  - (c)  $\langle a \rangle = \{a^0, a^1, \dots, a^{r-1}\}$  has exactly  $r$  elements;
  - (d) the subgroup  $\langle a \rangle$  is isomorphic to the cyclic group  $(\mathbb{Z}_r, +, -, 0)$ .

### 3. Cyclic groups

The **order** of an element  $a$  of a group  $G$ , denoted  $\text{ord}_G(a)$ , is the order of the subgroup generated by  $a$ .

**Theorem 3** Let  $(G, \cdot, ', e)$  be a group and  $a \in G$  be an element of finite order. Then:

- (1)  $\text{ord}_G(a) = \min\{r \geq 1 \mid a^r = e\}$ ;
- (2) if  $G$  is finite, then  $\text{ord}_G(a) \mid |G|$ ;
- (3)  $(\forall s \in \mathbb{Z})(a^s = e \Leftrightarrow \text{ord}_G(a) \mid s)$ ;
- (4) if  $G$  is finite, then  $a^{|G|} = e$ ;
- (5)  $(\forall s, t \in \mathbb{Z})(a^s = a^t \Leftrightarrow s \equiv t \pmod{\text{ord}_G(a)})$ ;
- (6)  $(\forall t \in \mathbb{Z})(\text{ord}_G(a^t) = \text{ord}_G(a) / (t, \text{ord}_G(a)))$ ;
- (7) if  $\text{ord}_G(a) = r_1 r_2$  and  $r_1, r_2 > 1$ , then  $\text{ord}_G(a^{r_1}) = r_2$ .



### 3. Cyclic groups

**Corollary 2** Let  $(G, \cdot, ', e)$  be a group and  $a, b \in G$  be elements of finite order. If  $a$  and  $b$  commute and  $(\text{ord}_G(a), \text{ord}_G(b)) = 1$ , then  $\text{ord}_G(ab) = \text{ord}_G(a)\text{ord}_G(b)$ .

**Theorem 4** Let  $(G, \cdot, ', e)$  be a finite group and  $a \in G$ . Then,

- (1)  $G = \langle a \rangle$  iff  $\text{ord}_G(a) = |G|$ ;
- (2)  $a$  generates  $G$  iff  $a^{|G|/q} \neq e$ , for any prime factor  $q$  of  $|G|$ ;
- (3) if  $a$  is a generator of  $G$ , then for any  $t \in \mathbb{Z}$ ,  $a^t$  is a generator of  $G$  iff  $(t, |G|) = 1$ ;
- (4) if  $G$  is cyclic, then it has  $\phi(|G|)$  generators.

## 4. The group $\mathbb{Z}_m^*$

Let  $m \geq 1$ . Recall that

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

and  $(\mathbb{Z}_m^*, \cdot, ^{-1}, 1)$  is a commutative group. Moreover,  $|\mathbb{Z}_m^*| = \phi(m)$ .

Given  $a \in \mathbb{Z}_m^*$ , denote

$$\text{ord}_m(a) = \text{ord}_{\mathbb{Z}_m^*}(a).$$

$\text{ord}_m(a)$  is called the **order of  $a$  modulo  $m$** .

When  $\mathbb{Z}_m^*$  is a cyclic group, its generators are also called **primitive roots modulo  $m$** .

## 4. The group $\mathbb{Z}_m^*$

Directly from Theorem 3 we obtain the following properties.

**Proposition 5** Let  $m \geq 1$  and  $a \in \mathbb{Z}_m^*$ . Then:

- (1)  $\text{ord}_m(a) = \min\{k \geq 1 \mid a^k \equiv 1 \pmod{m}\}$ ;
- (2) if  $a^k \equiv 1 \pmod{m}$ , then  $\text{ord}_m(a) \mid k$ . In particular,  $\text{ord}_m(a) \mid \phi(m)$ ;
- (3)  $\text{ord}_m(a) = \phi(m)$  iff  $a^{\phi(m)/q} \not\equiv 1 \pmod{m}$ , for any prime factor  $q$  of  $\phi(m)$ ;
- (4)  $a^k \equiv a^l \pmod{m}$  iff  $k \equiv l \pmod{\text{ord}_m(a)}$ ;
- (5)  $a^0 \pmod{m}, a^1 \pmod{m}, \dots, a^{\text{ord}_m(a)-1} \pmod{m}$  are pairwise distinct;
- (6)  $\text{ord}_m(a^k \pmod{m}) = \text{ord}_m(a) / (k, \text{ord}_m(a))$ , for any  $k \geq 1$ ;
- (7) if  $\text{ord}_m(a) = d_1 d_2$ , then  $\text{ord}_m(a^{d_1} \pmod{m}) = d_2$ .

## 4. The group $\mathbb{Z}_m^*$

**Corollary 3** Let  $m \geq 1$  and  $a, b \in \mathbb{Z}_m^*$ . If  $\text{ord}_m(a)$  and  $\text{ord}_m(b)$  are co-prime, then  $\text{ord}_m(ab \bmod m) = \text{ord}_m(a)\text{ord}_m(b)$ .

**Proposition 6** Let  $m \geq 1$  and  $a \in \mathbb{Z}_m^*$ . Then:

(1)  $a$  is a primitive root modulo  $m$  iff  $\text{ord}_m(a) = \phi(m)$ ;

(2)  $a$  is a primitive root modulo  $m$  iff

$$(\forall q)(q \text{ prime factor of } \phi(m) \Rightarrow a^{\phi(m)/q} \not\equiv 1 \bmod m);$$

(3) if  $a$  is a primitive root modulo  $m$ , then, for any  $k \geq 1$ ,  $a^k$  is a primitive root modulo  $m$  iff  $(k, \phi(m)) = 1$ ;

(4) if there are primitive roots modulo  $m$ , then there are exactly  $\phi(\phi(m))$  primitive roots.

## 4. The group $\mathbb{Z}_m^*$

**Theorem 5** There are primitive roots modulo  $m$  iff  $m = 1, 2, 4, p^k, 2p^k$ , where  $p \geq 3$  is a prime number and  $k \geq 1$ .

### Example 4

- There are primitive roots modulo 50 because  $50 = 2 \cdot 5^2$ .  
Moreover, there are  $\phi(\phi(50)) = \phi(20) = 8$  primitive roots modulo 50.
- There is no primitive root modulo 150.

## 5. The discrete logarithm problem

If  $G$  is a finite cyclic group and  $a$  is a generator of  $G$ , then

$$G = \{a^0 = e, a^1, \dots, a^{|G|-1}\}.$$

Given  $b \in G$ , there exists  $k < |G|$  such that  $b = a^k$ .  $k$  is called the **index of  $b$  w.r.t.  $a$**  or the **discrete logarithm of  $b$  to base  $a$** . When  $G = \mathbb{Z}_m^*$ ,  $k$  is called the **discrete logarithm of  $b$  to base  $a$  modulo  $m$**  and it is usually denoted by  $\log_a b \bmod m$ .

### Discrete Logarithm Problem (DLP)

Instance: finite cyclic group  $G$ , generator  $a$  of  $G$ , and  $b \in G$ ;

Question: find  $k < |G|$  such that  $b = a^k$ .

# 5. The discrete logarithm problem

## Facts:

- No efficient algorithm for computing general discrete algorithms is known;
- The naive approach is to raise  $a$  to powers  $i$  until the desired  $b$  is found (this method is sometimes called **trial multiplication**). The complexity of this method is linear in the size of the group and, therefore, it is exponential in the number of bits of the size of the group;
- While computing discrete logarithms is apparently difficult, the inverse problem of discrete exponentiation is easy (polynomial). This asymmetry has been exploited in the construction of cryptographic schemes: ElGamal encryption and digital signature, Diffie-Hellman key exchange protocol etc.

## 6. Applications to cryptography

### ElGamal digital signature:

- let  $p$  be a (large) prime and  $\alpha$  be a primitive root in  $\mathbb{Z}_p^*$ ;

- $\mathcal{P} = \mathbb{Z}_p^*$ ;

- $\mathcal{S} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$ ;

- $\mathcal{K} = \{(p, \alpha, a, \beta) \mid a \in \mathbb{Z}_{p-1}, \beta = \alpha^a \bmod p\}$ ;

- for any  $K = (p, \alpha, a, \beta)$  and  $k \in \mathbb{Z}_{p-1}^*$ , and any  $x \in \mathbb{Z}_p^*$ ,

- the message  $x$  is signed by

$$\text{sig}_K(x, k) = (\gamma, \delta),$$

where  $\gamma = \alpha^k \bmod p$  and  $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$

- the verification of the signature  $(\gamma, \delta)$  for  $x$  is performed by

$$\text{ver}_K(x, (\gamma, \delta)) = 1 \iff \beta^\gamma \gamma^\delta \equiv \alpha^x \bmod p;$$

- $p, \alpha$  and  $\beta$  are public, and  $a$  and  $k$  are secret.



## 6. Applications to cryptography

**Example 5** Let  $p = 467$ ,  $\alpha = 2$ , and  $a = 127$ . Then,

$$\beta = \alpha^a \bmod p = 2^{127} \bmod 467 = 132.$$

Assume that we want to sign  $x = 100$  using  $k = 213$  ( $k \in \mathbb{Z}_{466}^*$  and  $k^{-1} = 431$ ). Then:

$$\gamma = 2^{213} \bmod 467 = 29,$$

and

$$\delta = (100 - 127 \cdot 29) \cdot 431 \bmod 466 = 51.$$

Therefore,  $\text{sig}_K(x, k) = (29, 51)$ .

In order to verify the signature we compute

$$132^{29} \cdot 29^{51} \bmod 467 \quad \text{and} \quad 2^{100} \bmod 467$$

and accept the signature if they are equal.

## 6. Applications to cryptography

**Attack:** If the secret value  $k$  is used to sign two distinct messages  $x_1$  and  $x_2$ , then the secret parameter  $a$  could be easily computed.

Let  $\text{sig}_K(x_1) = (\gamma, \delta_1)$  and  $\text{sig}_K(x_2) = (\gamma, \delta_2)$  (the same  $k$  has been used). Therefore,

$$\beta^\gamma \gamma^{\delta_1} \equiv \alpha^{x_1} \text{ mod } p$$

and

$$\beta^\gamma \gamma^{\delta_2} \equiv \alpha^{x_2} \text{ mod } p,$$

which lead to

$$\alpha^{x_1 - x_2} \equiv \gamma^{\delta_1 - \delta_2} \text{ mod } p.$$

Because  $\gamma = \alpha^k \text{ mod } p$ , we get

$$\alpha^{x_1 - x_2} \equiv \alpha^{k(\delta_1 - \delta_2)} \text{ mod } p,$$

## 6. Applications to cryptography

which is equivalent to

$$k(\delta_1 - \delta_2) \equiv x_1 - x_2 \pmod{p-1}.$$

The solutions modulo  $p-1$  to this equation are of the form

$$(k_0 + i(p-1)/d) \pmod{p-1},$$

where  $k_0$  is an arbitrary solution,  $d = (\delta_1 - \delta_2, p-1)$ , and  $0 \leq i < d$ .  $k_0$  can be obtained by the extended Euclidean algorithm, and  $k$  can be obtained by checking the equation  $\gamma \equiv \alpha^k \pmod{p}$ .

If  $k$  is recovered, then the parameter  $a$  can be easily recovered from the equation  $\delta = (x - a\gamma)k^{-1} \pmod{p-1}$ , and the signature scheme is broken.

## 6. Applications to cryptography

- **Digital Signature Standard (DSS)** is the American standard for digital signatures;
- DSS was proposed by NIST in 1991, and adopted in 1994;
- DSS is a variation of the ElGamal digital signature. This variation is based on the following remark: the prime  $p$  in the ElGamal digital signature should be a 512-bit or 1024-bit number in order to ensure security. This fact leads to signatures that are too large to be used on smart cards;
- DSS modifies ElGamal digital signature so that the computations are done in a subgroup  $\mathbb{Z}_q$  of  $\mathbb{Z}_p^*$  by using an element  $\alpha \in \mathbb{Z}_p^*$  of order  $q$ .

## 6. Applications to cryptography

### Digital Signature Standard (DSS)

- let  $p$  a prime,  $q$  a prime factor of  $p - 1$ , and  $\alpha$  an element of order  $q$  in  $\mathbb{Z}_p^*$ ;
- $\mathcal{P} = \mathbb{Z}_p^*$ ;
- $\mathcal{S} = \mathbb{Z}_q \times \mathbb{Z}_q$ ;
- $\mathcal{K} = \{(p, q, \alpha, a, \beta) \mid a \in \mathbb{Z}_q \wedge \beta = \alpha^a \bmod p\}$ ;
- for any  $K = (p, q, \alpha, a, \beta)$  and  $k \in \mathbb{Z}_q^*$ , and any  $x \in \mathbb{Z}_p^*$ ,
  - $\text{sig}_K(x, k) = (\gamma, \delta)$ , where  $\gamma = (\alpha^k \bmod p) \bmod q$  and  $\delta = (x + a\gamma)k^{-1} \bmod q$ ;
  - $\text{ver}_K(x, (\gamma, \delta)) = 1 \iff (\alpha^{e_1} \beta^{e_2} \bmod p) \bmod q = \gamma$ , where  $e_1 = x\delta^{-1} \bmod q$  and  $e_2 = \gamma\delta^{-1} \bmod q$ ;
- $p, q, \alpha$ , and  $\beta$  are public, and  $a$  is secret.

## 6. Applications to cryptography

### Computing primitive roots:

Recall that an element  $\alpha \in \mathbb{Z}_m^*$  is a primitive root modulo  $m$  iff  $\alpha^{\phi(m)/q} \not\equiv 1 \pmod{m}$ , for any prime factor  $q$  of  $\phi(m)$ .

If  $p = 2q + 1$  and  $p$  and  $q$  are primes, then  $\alpha \in \mathbb{Z}_p^*$  is a primitive root modulo  $p$  iff  $\alpha^2 \not\equiv 1 \pmod{p}$  and  $\alpha^q \not\equiv 1 \pmod{p}$ . Moreover, there are  $\phi(\phi(p)) = q - 1$  primitive roots modulo  $p$ , which shows that the probability that a randomly generated number  $\alpha \in \mathbb{Z}_p^*$  is a primitive root is approximately  $1/2$ .

If  $\alpha$  is a primitive root modulo a prime  $p$  and  $q$  is a prime factor of  $p - 1$ , then  $\alpha^{\frac{p-1}{q}} \pmod{p}$  is an element of order  $q$ .