PQC Group-based Cryptography

Delaram Kahrobaei

The City University of New York

In this lecture we give an introduction to groups. We will bring examples and important theorem that we will use during the course.
An algebraic structure is a nonempty set together with one or more binary operations on that set.
Algebraic structures whose binary operations satisfy particularly important properties are semigroups, groups, rings, fields, modules, and so on. There are many books has written in this subject.

The objective of this section is to gibe the main definition of a group and bring known examples.

A group could be defined a semigroup with identity in which every element has a unique inverse. More formally:
Definition: A group is a non-empty set G, together with a binary operation $*$ such that the following axiom hold:

1. **Closure** G is closed under the operation $*$ if for every elements $x, y \in G$ then $x * y \in G$.
2. **Associativity** G is associative under the operation $*$ if for every elements $x, y, z \in G$ then $(x * y) * z = x * (y * z)$.
3. **Identity** There exists a unique element $e \in G$ (called the identity of G) such that for every element $x \in G$ then we have: $e * x = x * e$.
4. **Inverses** For every element $x \in G$ there exists a unique element $x^{-1} \in G$ (namely the inverse of x) such that $x * x^{-1} = x^{-1}x = e$.

Remark: It is common to omit $*$ altogether and write $x * y$ as xy which is called the product of x and y. The identity element of G can be also written as 1.
A group G is called abelian or commutative if for every element $x, y \in G$ we have $xy = yx$. In other words if the operation is commutative.

We definite the order of a group as follows:
Definition: The number of element of the group G is called the order of G and is denoted by $|G|$ or sometimes $o(G)$. The order of the group could be finite or infinite.

The basic goal of group theory is to classify groups. The easy fact but rather still important fact is that groups of same order may still be different. But also sometimes groups may seem different but still be the same.

Example: Let H_1 be the multiplicative group over the set $\{1, -1\}$, and let H_2 be the additive group of over the set $\{0, 1\}$ modulo 2. We see that the multiplicative table of these two groups differ only by name.

$\cdot$	1	-1
1	1	-1
-1	-1	1

Table: The multiplicative table of H_1

$+$	0	1
0	0	1
1	1	0

Table: The multiplicative table of H_2

Here we give formal definition of homomorphism and isomorphism to make this more formal. **Definition:** Let $(G, *)$ and $(H, \circ)$ be two groups. We say that G and H are isomorphic if there exists a bijection $f : G \to H$ such that for all $x, y \in G$ we have

$$f(x * y) = f(x) \circ f(y).$$

In other words such that the bijection f agrees with their structures. f is called an isomorphism and we denote the isomorphism of G and H by $G \cong H$.

Isomorphic groups look the same, we can obtain one group by renaming the elements of the other group. We leave it to the reader to prove that $\cong$ is an equivalent relation.

We we will bring some examples of groups.
Integers modulo n **under addition** Consider $(\mathbb{Z}_n, +)$. This forms an abelian group.
Integers modulo n **under multiplication** Consider $(\mathbb{Z}_n, \cdot)$. This forms semigroup but not a group. However if you consider $\mathbb{Z}_n{}^* = \mathbb{Z}_n \backslash \{0\}$. $\mathbb{Z}_n{}^*$ is a group under multiplication if and only if n is a prime.

The $(\mathbb{Z}, +)$, the set of interges under addition, $(\mathbb{Q}, +)$ the set of rationals under addition, $(\mathbb{R}, +)$ the set of reals under addition all form abelian groups.
None of the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ form a group under multiplication.
Removing 0 from the set of rationals $\mathbb{Q}$ and reals $\mathbb{R}$ form groups under multiplication.

Suppose $\mathbb{F}$ is a field (abelian group under both addition and multiplication). Typically $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Z}_p$ (where p is a prime number) are considered. Let $n \geq 2$, and consider the set of all $n \times n$ matrices with entries from $\mathbb{F}$. From Linear Algebra we know that the set of matrices under multiplication is associative. If I is the identity matrix, with ones on the diagonal and zeros elsewhere, then I is the identity element for the multiplication.

General Linear Groups, $GL(n, \mathbb{F})$: If we consider the of $n \times n$ matrices over the field $\mathbb{F}$, which have inverses, namely the ones that have determinant non-zero. Then this set forms a group under multiplication and is called the general linear group of dimension n over $\mathbb{F}$. It is denoted by $GL(n, \mathbb{F})$.
$GL(n, \mathbb{F})$ is an example of a non-abelian group.

Special Linear Groups, $SL(n, \mathbb{F})$: Consider the subset of $SL(n, \mathbb{F})$ of $GL(n, \mathbb{F})$ the set of matrices of determinant 1. Then $SL(n, \mathbb{F})$ forms a group under multiplication and is called the special linear group.

Definition: Let $(G, \cdot)$ be a group and H a subset of G. If H is a group relative to the binary operation of G, then we say H is a subgroup of G and we denote it by $H \leq G$.
Example: Every group G is the subgroup of itself. If e is the identity element of the group G then $\{e\}$ is the trivial subset of G.

Example: For the group of numbers we have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.
Theorem: If H is a non-empty subset of the group G, then the following three conditions are equivalent:

1. $H \leq G$.
2. For all elements x, y is in H, $xy \in H$ and $x^{-1} \in H$.
3. For all $x, y \in H$ we have $x^{-1}y \in H$.

Theorem: (Lagrange) The order of any subgroup of a finite group divides the order of the group.
Corollary Let G be a finite group of order n. Then for every element $x \in G$ we have $x^n = e$, where e is the identity element of the group G.

In this section, we introduce a way to present a group without list of its elements.

Definition: Generators: Let X be a subset of a group G. Let $H_i \leq G$ (where $i \in I$ is an indexed set) which contain the set X. Then $\langle X \rangle = \bigcap_{i \in I} H_i \leq G$ is the smallest subgroup generated by X.

The following theorem states the practical way of calculating the elements of a subgroup, given a generating set X.
Theorem: Let X be a subset of a group G. Then the subgroup generated by X, namely $\langle X \rangle$ consists of all possible products of elements in X and their inverses.

Definition: A group is called cyclic if it can be generated by a single element.

Theorem: Let G be a cyclic group. Then one of the following conditions hold:

1. If G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$.
2. If G is finite of order n, then G is isomorphic to $(\mathbb{Z}_n, +)$ or $(\mathbb{Z}_n{}^*, \cdot)$.

Definition

Let H be a subgroups of a group G, $H \leq G$. Given an element $a \in G$. We define the left coset of H in G determined by a as follows

$$aH = \{ah | h \in H\}.$$

The corresponding right coset of H in G determined by a is $Ha = \{ha | h \in H\}$.

Definition

Let G be a group and N be a subgroup of G ($N \leq G$). If for every $x \in G$ we have $xNx^{-1} \subset N$ then N is said to be normal. It is denoted by $N \triangleleft G$.

Example

If G is a group. Then the following is true

- The trivial subgroup $\{e\}$ is normal in G.
- $G \triangleleft G$.

Example

Let G be an abelian group. Then every subgroup H of G is normal in G, $H \triangleleft G$. But the converse is not necessarily true.

Theorem

Let G be a group. N is a normal subgroup of G if and only if any right coset of N in G is also a left coset of N in G for every $x \in G$, $xN = Nx$.

Definition

Let N be a normal subgroup of a group G. We denote the set of all cosets of N in G by G/N and we say G/N is the factor group or the quotient group.

Theorem

Let G be a group and $N \triangleleft G$ then the quotient group G/N is a group under the binary operation:

$$(xN)(yN) = (xy)N.$$

Example

The special linear group is a normal subgroup of the general linear group.

$$SL(n, \mathbb{F}) \triangleleft GL(n, \mathbb{F}).$$

Let F be a group, with generating set X. If every element of F can be written uniquely as a product of elements X and their inverses, then we say F is a free group. Here we bring a more precise definition of a free group.

Definition

Let X be a set, and we call X an alphabet and its elements letters. We define a word over X to be a finite sequence of letters and their formal inverses. The empty word that we denote it by e is the empty sequence. If a word w does not contain a subword of the form xx^{-1} or $x^{-1}x$ for all $x \in X$, we we call w a reduced word. We denote the set of all reduced words in the set of alphabet X, by $F(X)$. $F(X)$ forms a group under multiplication and is called the free group on X.

Example

Let $X = \{x, y\}$ be the set of alphabet. Then x and y are letters of X and

$$xy, y, xyxyx, x^{-1}yxy^{-1}, xy^{-1}xx^{-1}y$$

are examples of words over X. The first four words are examples of reduced words.

Example

The infinite cyclic group is a free group of rank 1, because it can be generated by one element.

Presentations are ways of defining groups as quotient of free groups.

Definition

Let X be an alphabet. A relation over X is any par (w, w') of reduced words over X. We usually write $w = w'$ instead of (w, w'). Note that $ww'^{-1} = 1$ (where 1 denoted the identity). Let R be the set of all relations. We define a presentation as a pair

$$\langle X; R \rangle.$$

Definition

Let $F(X)$ be the free group on the set X. Define N to be the smallest normal subgroup of $F(X)$ containing the set $\{ww'^{-1}|(w = w') \in R\}$. Then the group defined by a presentation $\langle X; R\rangle$ is the quotient $F(X)/N$.

Example

The free group $F(X)$, generated by X of rank $|X|$ has the following presentation $\langle X; \rangle$

Example

The cyclic group of order $n \in \mathbb{N}$ has the following presentation

$$\mathbb{Z}_n = \langle x; x^n = 1 \rangle.$$

Example

For the abelian group generated by a and b, we have the following presentation

$$\langle a, b; a^{-1}b^{-1}ab = 1 \rangle$$

Definition

Let G be a group presented by $\langle X; R \rangle$. G is said to be finitely generated if $|X|$ is finite. G is called finitely presented if it is finitely generated and $|R|$ is finite.

Example

- All finite groups are finitely presented.
- Cyclic groups are finitely presented.
- Free groups of finite rank are finitely presented.

Here we first bring an example of a nilpotent group of class 2, namely Heisenberg group. Then we will define what a nilpotent group is.

Definition

The commutator of two elements x and y is denoted by $[x, y]$ and is equal to

$$[x, y] = x^{-1}y^{-1}xy.$$

Definition

Heisenberg group: Let $r, s, t \in \mathbb{Z}$, now consider the group H of the matrices of the form

$$\begin{pmatrix} 1 & r & s \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$$

Define A, B and C as follows:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

One can check for all $k, l, m \in \mathbb{Z}$, the following holds:

$$A^k = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B^l = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix}, C^m = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Each element of H is then equal to one of the matrices:

$$A^k B^l C^m = \begin{pmatrix} 1 & k & m+kl \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix}.$$

In view of relations

$$[A, B] = C, [C, A] = [C, B] = I_3$$

So we propose the following presentation for H:

$$H = \langle a, b, c; [a, b] = c, [c, a] = [c, b] = 1 \rangle$$

Definition

Let G be a group and A, B be two subgroups of G. We define $[A, B]$ to be the subgroup of G generated by all commutators $[a, b]$ such that $a \in A, b \in B$.

Definition

Define inductively a series of subgroup $\gamma_i(G)$, $i = 0, 1, \cdots$ as follows:

$$\gamma_0(G) = G, \gamma_{i+1}(G) = [\gamma_i(G), G].$$

A group G is nilpotent of class m if for some m, $\gamma_m(G) = \{e\}$.

Lemma

One can show that $\gamma_{i+1}(G) \leq \gamma_i(G)$.

Theorem

The Heisenberg group is nilpotent of class 2.

Definition

Let G be a group, G is called metacyclic, if there exists a normal subgroup $N \triangleleft G$ such that both G/N and N are cyclic groups.

Example

Consider the group which has the following presentation

$$G = \langle x, y; x^m = 1, y^{-1}xy = x^r, y^n = x^s (m, n, r, s \in \mathbb{N}(r, s \leq m)) \rangle$$

Then $N = \langle x \rangle$ is a normal subgroup of G such that

$$N \cong \mathbb{Z}_m, G/N \cong \mathbb{Z}_n$$

Therefore G is a finite metacyclic group, and every metacyclic group has a presentation of this form.

Definition

Let G be a group, G is called metacyclic, if there exists a normal subgroup $N \triangleleft G$ such that both G/N and N are cyclic groups.

Example

Consider the group which has the following presentation

$$\begin{aligned} G \quad = \quad & \langle x, y; x^m = 1, y^{-1}xy = x^r, y^n = x^s \\ & (m, n, r, s \in \mathbb{N}(r, s \leq m), r^n \equiv 1, rs \equiv s(mod m))\rangle \end{aligned}$$

Then $N = \langle x \rangle$ is a normal subgroup of G such that

$$N \cong \mathbb{Z}_m, G/N \cong \mathbb{Z}_n$$

Therefore G is a finite metacyclic group, and every metacyclic group has a presentation of this form.

Definition

A group is called polycyclic if there exists a polycyclic series through the group; i.e. a subnormal series of finite length with cyclic factors

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

such that G_{i+1}/G_i is cyclic.

Example

Every finitely generated nilpotent or abelian group is polycyclic.

Example

The Dihedral group of order 8, D_8 is a finite polycyclic group.

Theorem

Every polycyclic group has a finite presentation which exhibits the polycyclic structure of the considered group: a polycyclic presentation of the form

$$\langle a_1, \ldots, a_n; a_j^{a_i} = w_{ij}, a_j^{a_i^{-1}} = v_{ij}, a_k^{r_k} = u_{kk} \text{ for } 1 \leq i < j \leq n \text{ and } k \in I \rangle$$

where $I \subseteq \{1, \cdots, n\}$ *and* $r_i \in \mathbb{N}$ *if* $i \in I$ *and the right hand sides* w_{ij}, v_{ij}, u_{jj} *of the relations are words in the generators* $a_{j+1}, \cdots, a_n$.

Definition

Normal Form Using induction, it is straightforward to show that every element in the group defined by this presentation can be written in the form

$$a_1^{e_1} \cdots a_n^{e_n}$$

with $e_i \in \mathbb{Z}$ and $0 \leq e_i < r_i$ if $i \in I$.

Example

The following a presentation of a polycyclic group:

$$G := \langle x_1, x_2, x_3; {x_1}^3 = x_3, {x_2}^2 = x_3, {x_1}^{-1} x_2 x_1 = x_2 x_3, x_1 x_2 {x_1}^{-1} = x_2 x_3 \rangle$$

Example

The following a presentation of a polycyclic group:

$$G := \langle x_1, x_2; {x_1}^2 = 1, x_1 x_2 {x_1}^{-1} = {x_2}^{-1}, {x_1}^{-1} x_2 x_1 = {x_2}^{-1} \rangle$$

Prove the following statements:

- Let F_1 and F_2 be free groups with bases X_1 and X_2. Then F_1 and F_2 are isomorphic if and only if X_1 and X_2 have the same cardinal.

- Consider the group which has the following presentation

$$\begin{aligned} G &= \langle x, y; x^m = 1, y^{-1}xy = x^r, y^n = x^s \\ &\quad (m, n, r, s \in \mathbb{N}(r, s \leq m), r^n \equiv 1, rs \equiv s(mod m))\rangle \end{aligned}$$

Then $N = \langle x \rangle$ is a normal subgroup of G such that

$$N \cong \mathbb{Z}_m, G/N \cong \mathbb{Z}_n$$

Therefore G is a finite metacyclic group, and every metacyclic group has a presentation of this form.