Lecture Notes for Abstract Algebra: Lecture 4

1 Groups and examples

1.1 Groups

Definition 1. Let X be a set with a binary operation $*: X \times X \longrightarrow X$. The set X, together with the operationa $*$, is a group if:

(i) There exist a neutral element $e \in X$ such that $e * x = x * e = x$ for all $x \in X$.

(ii) The operation is associative $(x * y) * z = x * (y * z)$ for all $x, y, z \in X$.

(iii) There exist an inverse: for all $x \in X$, there exist $x' \in X$ such that $x * x' = x' * x = e$.

A group is said to be abelian or commutative when we have the extra condition (iv) $x * y = y * x$, for all elements $x, y \in S$.

Remark 2. A group is not empty. It has at least a neutral element e.

Remark 3. A set X with a binary operation $*: X \times X \longrightarrow X$, satisfying only (i) and (ii) is called a monoid. A group, is then, a monoid where every element has an inverse. For instance, the naturals $\mathbb{N}$ with multiplication with identity 1, is a monoid but not a group.

Example 4. Some examples of groups:

- (Vector spaces) A vector space $(V, +)$ with addition of vectors as operation, is a commutative group. In fact, a commutative group $(A, +)$ behave like a vector space over $\mathbb{Z}$. (Vector spaces with multiplication is not a group, because the operation gives scalar not vectors).

- (Cyclic group of order n) The group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, of integers with addition mod n, is an abelian group. This group is also referred to as: The cyclic group of order n and is also denoted by C_n.

- (Multiplicative group of units in $\mathbb{Z}_n$) Elements of $\mathbb{Z}_n$ admitting a multiplicative inverse are called units of $\mathbb{Z}_n$. A non-zero element $k \in \mathbb{Z}_n$ admits inverse if and only the $\gcd(k, n) = 1$. These elements form a group of order $\varphi(n)$ called $U(n)$.

- (Group of n-roots of unity) Let $n > 1$ and consider the multiplicative set of complex roots $\Phi_n = \{\xi \in \mathbb{C} \,|\, \xi^n = 1\}$. This is also an abelian group.

- (Symmetric group) Let S be a set of n elements. The symmetric group S_n is the group of bijective maps $S \longrightarrow S$ with composition. S_n is non-abelian for $n > 2$.

- (General linear group over $\mathbb{R}$) The general linear group is the group $\mathrm{GL}_n(\mathbb{R})$ of invertible matrices ($\det \neq 0$), with matrix multiplication. $\mathrm{GL}_n(\mathbb{R})$ is non-abelian for $n > 1$. As a generalization, we can take the group $\mathrm{GL}(V)$ of automorphisms on a vector space V (non-necessarily of finite dimension). The definition of $\mathrm{Gl}_n(\mathbb{R})$ is based on the property $\det(A \cdot B) = \det(A)\det(B)$.

- (The special linear group) The special linear group $\mathrm{SL}_n(\mathbb{R})$ or $\mathrm{SL}(n, \mathbb{Z})$ of matrices with determinant 1. Also non abelian for $n > 1$.

- (The dihedral group) The group $\mathbb{D}_n$ of symmetries on the regular polygon of n sides. As with the symmetric group, we use composition of maps as operation for the group. The groups $\mathbb{D}_n$ are non-abelian for $n > 2$.

- (The Quaternions Q_8) As a generalization of the group $\{\pm 1, \pm i\}$ of fourth roots of unity, consider the group

  $$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, \quad \text{where} \quad i^2 = j^2 = k^2 = -1 = i * j * k.$$

  It can be checked $i * j = k$, $j * k = i$, $k * i = j$, $j * i = -k$, $i * k = -j$ and $k * j = -i$. This group is called the Quaternion group and is not commutative. For a matrix representation of Q_8, see Judson page 42 Ex 3.15.

- (Direct product of groups) Given groups $(G, *)$ and $(H, .)$, we can construct a group that is the direct product of G and H. As a set, the direct product is just the Cartesian product $G \times H$ together with the operation

  $$(g, h)(g', h') = (g * g', h.h').$$

  The group $G \times H$ is called the external direct product of G and H.

- (Galois group of an extension) Suppose that F is a field and E/F is an extension, we can build the group of F-automorphism of E:

  $$\mathrm{Gal}(E/F) = \{\sigma\colon E \longrightarrow E \mid \sigma(x) = x \ \forall \ x \in F\}.$$

  The operation on automorphisms being compositions of maps. For a polynomial $p(x)$ with coefficients in the field F, we can consider the splitting field E_p, where p factors completely and the Galois group of the polynomial as $\mathrm{Gal}(E_p/F)$.

Proposition 5. *Let G be a group. Then, we have the following properties:*

(1) The neutral element is unique.

(2) The inverse x^{-1} of x is unique.

(3) For any elements $a, b \in G$, the equations $a * x = b$ and $x * a = b$ have unique solutions in G.

(4) The inverse $(a*b)^{-1}$ of the element $a*b$ is the element $b^{-1}*a^{-1}$.

Proof. We proceed to do each of the points:
(1) Suppose that we have neutral elements e and e', then $e = e*e' = e'$.
(2) Suppose that x has two inverses x' and x'', then

$$x' = e*x' = (x''*x)*x' = x''*(x*x') = x''*e = x''.$$

(3) The solutions are $x = a^{-1}*b$ and $x = b*a^{-1}$ respectively.
(4) $b^{-1}*a^{-1}*a*b = e$ and $a*b*b^{-1}*a^{-1} = e$. □

Remark 6. Let G be a group and $x \in G$. The three most important actions that we can build in G:

(1) Left multiplication: $f_x\colon G \longrightarrow G$, given by $f_x(y) = x*y$.

(2) Right multiplication: $g_x\colon G \longrightarrow G$, given by $f_x(y) = y*x$.

(3) Conjugation: $\varphi_x\colon G \longrightarrow G$, given by $\varphi_x(y) = xyx^{-1}$.

Corollary 7. *Left multiplication, right multiplication and conjugation by an element are bijective maps $G \longrightarrow G$.*

1.2 Cayley tables. Example of groups: $\mathbb{D}_3$, the symmetries on the equilateral triangle

A symmetry of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles. Consider, for example, an equilateral triangle labeled $\{A, B, C\}$ and the rigid motions:

$$\rho_1 = \text{ rotation counterclockwise } 120° \text{ with barycenter as origin}, \quad \rho_2 = \rho_1^2, \quad \rho_3 = \rho_1^3 = id$$

$$\mu_1 = \text{ reflection about symmetry axis through vertex A}$$
$$\mu_2 = \text{ reflection about symmetry axis through vertex B}$$
$$\mu_3 = \text{ reflection about symmetry axis through vertex C}$$

There are some relations between these, for instance

$$\mu_1 \circ \rho_1 = \mu_2 \qquad \text{and} \qquad \rho_1 \circ \mu_1 = \mu_3.$$

The Cayley table of a group is a table aimed to represent the structure of a group. The Cayley table for $\mathbb{D}_3$ looks like:

$$\mathbb{D}_3 = \begin{array}{c|cccccc} & id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \hline id & id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \rho_1 & \rho_1 & \rho_2 & id & \mu_3 & \mu_1 & \mu_2 \\ \rho_2 & \rho_2 & id & \rho_1 & \mu_2 & \mu_3 & \mu_1 \\ \mu_1 & \mu_1 & \mu_2 & \mu_3 & id & \rho_1 & \rho_2 \\ \mu_2 & \mu_2 & \mu_3 & \mu_1 & \rho_2 & id & \rho_1 \\ \mu_3 & \mu_3 & \mu_1 & \mu_2 & \rho_1 & \rho_2 & id \end{array}$$

Some other finite groups with their Cayley tables are:

$$\mathbb{Z}_4 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \qquad \mathbb{V}_4 = \begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

$$\mathbb{Z}_2 = \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ a & 1 & 0 \end{array} \qquad \mathbb{Z}_3 = \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

Practice Questions:

1. Show that the direct product of two groups is a group.

2. Draw a diagram showing all 8 symmetries of a square.

3. Show that a non-zero element $k \in \mathbb{Z}_n$ admits inverse if and only the $\gcd(k, n) = 1$.