Lecture 5

Reference: Judson, Chapters 3.1

Units in $\mathbb{Z}_n$

Recall that $\mathbb{Z}_n$ is the set of congruence classes modulo n.

Remark 1: Convention on notation

Given a fixed integer n we will often identity an integer number $a \in \mathbb{Z}$ with the corresponding congruence class in $\mathbb{Z}_n$. For example we will write

$$5 \in \mathbb{Z}_7$$

assuming the congruence class of integers [5] modulo 7. In particular we can write

$$5 = 19 \text{ in } \mathbb{Z}_7$$

since 5 and 19 belong to the same congruence class.
This allows us, by abuse of notation, write

$$\mathbb{Z}_n = \{0, 1, 2 \ldots, n-1\}$$

instead of the formally correct

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

An element $k \in \mathbb{Z}_n$ is called a *unit*, if there exists an element $l \in \mathbb{Z}_n$ such that

$$k \cdot l = 1 \text{ in } \mathbb{Z}_n.$$

The following theorem provide a complete characterization of units in $\mathbb{Z}_n$.

Theorem 1: Characterization of units in $\mathbb{Z}_n$

Let $n \geqslant 2$ be an integer. The set of units in $\mathbb{Z}_n$ (denoted $\mathbb{Z}_n^\times$) consists of all congruence class of integers coprime to n:

$$\mathbb{Z}_n^\times = \{k \in \mathbb{Z}_n \mid \gcd(n,k) = 1\}$$

Proof. Let $k \in \{0, \ldots, n-1\}$.
1. If $\gcd(n,k) = 1$, then by the theorem from the previous week, we can find integers $u, v \in \mathbb{Z}$ such that

$$nu + kv = 1.$$

Therefore, in $\mathbb{Z}_n$ we have

$$k \cdot v \equiv 1 \mod n,$$

so that $[v]$ is the multiplicative inverse of $[k]$ in $\mathbb{Z}_n$.
2. Conversely, if we can find a multiplicative inverse to $[k] \in \mathbb{Z}_n$:

$$k \cdot l \equiv 1 \mod n,$$

then any common divisor of k and n would also divide 1, so necessarily $\gcd(n,k) = 1$. □

Example 1

In $\mathbb{Z}_6$ the only units are 1 and $5 = -1$.

Definition 1

Given integer $n \geqslant 2$, define *Euler's function* $\varphi(n)$ to be the number of integers in $\{1, \ldots, n-1\}$ which a coprime with n.

In other words,
$$|\mathbb{Z}_n^\times| = \varphi(n).$$

Problem 1: Number n is prime, if and only if $\varphi(n) = n-1$.

Groups

Laws of composition

Let S be an arbitrary set.

Definition 2: Law of composition

A *law of composition* (or *binary operation*) on S is a function
$$S \times S \to S$$
which assigns to any pair $(x,y) \in S \times S$ an element $x * y \in S$. (Instead of $x * y$ often we will write $x \cdot y$, or even xy)

Example 2

Addition and multiplication are composition laws on $\mathbb{Z}$.
Division is not a composition law on $\mathbb{R}$, since $x/0$ is not defined. However, it is a composition law on $\mathbb{R}\backslash\{0\}$.

Example 3: Important example

Let X be an arbitrary set, and consider
$$S = \mathcal{F}(X,X)$$
to be the set of all maps $f\colon X \to X$. Given a pair of maps $f, g \in \mathcal{F}(X,X)$, we can take their composition and obtain an element $f \circ g \in \mathcal{F}(X,X)$. Hence, the composition of maps defines a *law of composition* on $\mathcal{F}(X,X)$ (thus the name).

Definition 3

Let
$$S \times S \to S$$
$$(x,y) \mapsto x * y$$
be a law of composition on S. We say that $*$ is

- *associative*, if for any $x,y,z \in S$ we have
$$(x*y)*z = x*(y*z).$$
- *commutative*, if for any $x,y \in S$
$$x*y = y*x.$$

If the law of composition is associative, given $x_1, \ldots, x_n \in S$, it makes sense to write just
$$x_1 * x_2 * \cdots * x_k$$
without any brackets.

Traditionally, we drop the symbol $*$ and denote a law of composition by $(x,y) \mapsto xy$ (this is called the multiplicative notation), but if it happens to be commutative, the additive notation $(x,y) \mapsto x+y$ may be used. For the moment, for clarity, we will keep using the symbol $*$.

Definition 4

Let $(S,*)$ be a set with a composition law. We say that $e \in S$ is an *identity* (or *neutral element*) if for all $x \in S$ we have

$$x * e = e * x = x.$$

Problem 2: Any law of composition has at most one identity element.
Hint: given two identities e, e' consider $e * e'$.

Definition 5

Let $(S,*)$ be a set with a composition law with an identity e. We say that $y \in S$ is *invertible* if there exists $x \in S$ such that

$$x * y = y * x = e.$$

The inverse of y is denoted by y^{-1}.
Clearly, e is invertible with $e^{-1} = e$.

Proposition 1

Let $(S,*)$ be a set with an associative composition law and identity. Let $x, y \in S$ be two invertible elements, then $x * y$ is also invertible with $(x * y)^{-1} = y^{-1} * x^{-1}$

Proof. Indeed, we have

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$$

where in the first equality we used associativity, in the second the fact that y^{-1} is the inverse of y, in the third the property of the identity e, and in the last the fact that x^{-1} is the inverse of x.
Similarly we check that $(y^{-1} * x^{-1}) * (x * y) = e$ which proves that $(y^{-1} * x^{-1}) = (x * y)^{-1}$. □

Example 4: Key motivating example

Let Δ be an equilateral triangle. Then it has 6 symmetries:

- 3 rotations – by $0°$, $120°$ and $240°$ (denote them τ_0, τ_1, τ_2)
- 3 reflections along 3 altitudes (denote them by $\sigma_1, \sigma_2, \sigma_3$).

We claim that the composition operation on the set $\{\tau_0, \tau_1, \tau_2, \sigma_1, \sigma_2, \sigma_3\}$ defines a law of composition (exercise).

Problem 3: Prove that the above law of composition is associative, has an identity and every element admits an inverse.

Definition of a group

Definition 6

Let $(G,*)$ be a set with a law of composition. We will say that $(G,*)$ si a group if the following properties hold:

- $*$ is associative
- there is an identity $e \in G$
- every element $x \in G$ is invertible.