# Notes for 12 Feb (Tuesday)

## 1 The road so far...

1. Defined rings and fields and gave examples.

2. Defined a ring structure on $\mathbb{Z}/m\mathbb{Z}$

## 2 Rings and Fields

**Lemma 2.1.** *$[a]_m$ is a unit of $\mathbb{Z}/m\mathbb{Z}$ iff $gcd(a, m) = 1$.*

As a corollary, the number of units of $\mathbb{Z}/m\mathbb{Z}$ is simply the number of numbers $1 \leq a \leq m$ that are coprime to $m$. This number is denoted as $\phi(m)$. (The Euler totient function.) Calculating this function requires some machinery that we will develop later.

Def : A nonzero element $a$ of a commutative ring $R$ for which there is some $b$, also not zero, with $ab = 0$ is called a zero divisor. Note that $\mathbb{Z}/6\mathbb{Z}$ has zero divisors like $[2]_6$. It is easy to see that units cannot be zero divisors. (But please note that just because something is not a zero divisor does not mean it is a unit. For instance, $2 \in \mathbb{Z}$ is not a zero divisor but it is not a unit either.)

**Lemma 2.2.** *Let $R$ be a commutative ring and suppose $a \neq 0$ in $R$ is not a zero divisor. Then if $b, c \in R$ such that $ab = ac$, then $b = c$.*

*Proof.* Indeed, $a(b - c) = 0$ and hence $b = c$ because $a$ is not a zero divisor. □

As a corollary, if $a$ is not a zero divisor, then $ax = b$ has at most one solution. A commutative ring that has no non-trivial zero divisors is called an integral domain (or simply, a domain). Integers and polynomials are examples.

**Theorem 1.** *Let $R$ be an integral domain. For every $r, s \in R$, the equation $x^2 - rx + s = 0$ has at most two roots. On the other hand, if $R$ has complementary zero divisors $a, b \neq 0$, i.e., $ab = 0$, such that at least three of $0, a + b, a, b$ are distinct, then $x^2 - (a + b)x = 0$ has at least three roots in $R$.*

*Proof.* Let us prove that second part first : $x(x - (a + b)) = 0$. So $x = 0, a + b, a, b$ are roots. Three of these are distinct by assumption.
First part : Suppose $a, b, c$ are three distinct roots. Then $r(a - c) = a^2 - c^2 = (a + c)(a - c)$ and $r(b - c) = b^2 - c^2 = (b + c)(b - c)$. By cancellation, $r = a + c = b + c$ and hence $a = b$. A contradiction. □

The following theorem characterises units and zero divisors in $\mathbb{Z}/m\mathbb{Z}$.

**Theorem 2.** *In* $\mathbb{Z}/m\mathbb{Z}$

1. $[a]_m$ *is a unit if* $gcd(a, m) = 1$.
2. $[a]_m$ *is a zero divisor, if* $1 < gcd(a, m) < m$.
3. $[a]_m = [0]_m$ *if* $gcd(a, m) = m$.

*Proof.*

1. $ax \equiv 1 \ mod \ m$ can be solved for if $gcd(a, m) = 1$ (by Bezout's identity).
2. Note that $[m/gcd(a, m)]_m[gcd(a, m)]_m = [0]_m$.
3. Trivial.

□

As a corollary,

**Proposition 2.1.** $\mathbb{Z}/m\mathbb{Z}$ *is a field iff* $m$ *is a prime.*

*Proof.* If $m$ is a prime, then $gcd(a, m) = 1$ for all $a \neq 0$. Hence $a$ is a unit and $\mathbb{Z}/m\mathbb{Z}$ is a field.
If $\mathbb{Z}/m\mathbb{Z}$ is a field and $m = n_1n_2$, then $[n_1]_m[n_2]_m = [0]_m$, a contradiction unless $m$ is a prime. □