Math 122 – Lecture 20 Notes

1 Rings and Fields

$\mathbb{Z}/n\mathbb{Z}$ has $+, \cdot$, both of these operation are important, but so far we have not considered them "together", only as $(\mathbb{Z}/n\mathbb{Z}, +)$ and $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$. On the other hand, we noticed that;

$$Aut((\mathbb{Z}/n\mathbb{Z})^\times, \cdot) \to Aut(\mathbb{Z}/n\mathbb{Z}, +)$$

By element $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting as $x \to mx$ for $x \in Aut(\mathbb{Z}/n\mathbb{Z}, +)$, so that these operations are compatible in some sense.

What if we consider $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$?
Definition: A ring R is a set with $+ : R \times R \to R$ (addition) and $\cdot : R \times R \to R$ (multiplication) such that;

(a) $(R, +)$ is a commutative group, its identity is $0 \in R$

(b) $(R, \cdot)$ is a monoid, identity is 1, with $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $a \cdot 1 = a = 1 \cdot a$.

(c) Distributive Law: $\forall a, b, c \in R$, we have that

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$c \cdot (a + b) = c \cdot a + c \cdot b$$

Where we have homomorphisms that sends $x \in (R, +)$ to $c \cdot x \in (R, +)$, and $x \to x \cdot c$.

Remark: In general, people also consider rings without identity, $(R, \cdot)$ a semigroup, but we will not consider this generalization.

Examples of commutative rings are ;

$$\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

since $\cdot$ is commutative. An example of a noncommutative ring is a matrix;

$$\mathrm{Mat}_{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$$

We see that;

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

Exercise: Check that this is a noncommutative ring.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

So we see that it is not commutative. Note that for a ring R, then $R^\times$ is a group, with $R^\times = \{x \in R | \exists y \in R, xy = yx = 1\}$.

Important subclass of rings: R is a division ring (skew field) if $R^\times = R \setminus \{0\}$. We also have that R is a *field* if;
1) R is a division ring.
2) R is commutative.

Examples: $\mathbb{Z}$ is not a field, while;

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}$$

are fields.

Claim: $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.
Proof: $(\mathbb{Z}/n\mathbb{Z})^\times = \{k = 1, \cdots, n-1 | \gcd(k, n) = 1\}$ coincides with $\{1, \cdots, n-1\}$ if and only if n is prime.

Another example of rings:
For a ring R, define;

$$R[x] := \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 | a_i \in R\}$$

where x is the formal symbol, and $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a formal linear combination. For example, if $R = \mathbb{Z}$, then examples of elements of $\mathbb{Z}[x]$ are:

Polynomial	Degree	Leading Coefficient	Constant Term
5	0	5	5
$x + 5$	1	1	5
$3x^2$	2	3	0
$2x^{100} + 1$	100	2	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Terminology: If $f(x) \in R[x]$, then $\deg(f(x))$ is the largest n such that the coefficient in front of x^n in $f(x)$ is nonzero.
Leading term is the coefficient in front of x^n.
Constant term is a_0.

Operations on polynomials: Consider $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i$, where we have;
$+ : R[x] \times R[x] \to R[x]$;

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$$

Ex;

$$(2x + 3) + (x^2 + 8x + 4) = x^2 + 10x + 7$$

$\cdot : R[x] \times R[x] \to R[x]$;

$$f(x) \cdot g(x) = \sum_{i,j} a_i b_j \cdot x^{i+j} = \sum_k \Big(\sum_{i+j=k} a_i b_j \Big) x^k = (a_0 + a_1 x + a_2 x^2 + \cdots)(b_0 + b_1 x + b_2 x^2 + \cdots)$$

$$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots$$

Ex;

$$(3 + 2x)(4 + 8x + x^2) = 12 + (24 + 8)x + (3 + 16)x^2 + (21)x^3 = 2x^3 + 19x^2 + 32x + 12$$

Proposition: $(R[x], +, \cdot)$ is a ring.
Proof: Direct computation (exercise in the pset).

Roots of polynomials: Elements $p \in R[x]$ define functions $R \to R$;

$$\alpha \to p(\alpha) = a_0 + a_1 \cdot \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n$$

We then have that $\alpha \in R$ is a *root* of p if $p(\alpha) = 0$.

Example: $R = \mathbb{R}$, then $x^2 - 2$ has roots $\alpha = \pm\sqrt{2}$. $x^2 - 2x + 1$ has root 1.

We will prove the following theorem:

Theorem: If R is a field, $p \in R[x]$, then the number of roots of p is $\leq \deg p$.

Proof: Recall for $f, h \in \mathbb{Z}$, we have $f = q \cdot h + r$ with $0 \leq r < h$.
Division with remainder, $f(x), h(x) \in R[x]$, assume $h(x)$ is monic. Then $\exists! q(x), r(x) \in R[x]$ such that $f(x) = q(x) \cdot h(x) + r(x)$, so $\deg(r) < \deg(h)$.
Example: take $f(x) = 2x^3 + 3, h(x) = x^2 + 1$. We can then write;

$$f(x) = (2x^3 + 3) = (2x)(x^2 + 1) - 2x + 3$$

So we have $r(x) = -2x + 3$ and $q(x) = 2x$.

Proposition: $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (p-prime).