"Recall" 21.1

Definition A ring is an abelian group $(R, +, 0)$ together with a binary operation $\cdot$ so that

1) $\cdot$ is associative: $a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall\, a,b,c \in R$

2) $\cdot$ distributes over $+$:
$$a\cdot(b+c) = (a\cdot b) + (a\cdot c) \text{ and } (b+c)\cdot a = (b\cdot a) + (c\cdot a)$$
for all $a,b,c \in R$

We also require (and this is not universal) that our rings have "unity", ie $1_R \in R$ so that
$$a\cdot 1_R = a = 1_R\cdot a \qquad \forall a \in R$$

Notation (i) We'll omit $\cdot$ and write ab for $a\cdot b$

(ii) we'll omit R in 1_R and simply write 1.

Examples of rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n \ (n\geq 1)$

$M_n(\mathbb{R}) = n\times n$ real matrices

$M_n(\mathbb{Z}) = n\times n$ integral matrices

$M_n(\mathbb{C}) = n\times n$ complex matrices

Def A ring R is commutative if $\cdot$ is commutative:
$$a\cdot b = b\cdot a \qquad \forall a,b \in R$$

Ex $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ are commutative;
$M_n(\mathbb{R})$ $(n>1)$ is not.

Note By our definition $R = 2\mathbb{Z}$ is not a ring;
there is no $k \in 2\mathbb{Z}$ s.t. $ka = a = ak \quad \forall a \in 2\mathbb{Z}$

Many textbooks don't require that rings have 1.
(They are wrong, I think).

<u>Definition</u> An element u of a ring R is a <u>unit</u> (not to be confused with unity) if $\exists v \in R$ s.t. $u \cdot v = 1_R = v \cdot u$.

<u>Notation</u> $R^\times$ = the set of units of a ring R

$(R^\times, \cdot, 1_R)$ is a group.

<u>Ex</u> $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$

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

$M_n(\mathbb{Z})^\times = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$

(this is not completely obvious)

<u>Lemma 21.1</u> For any ring ring R, for any $a \in R$

$$a \cdot 0 = 0 = 0 \cdot a.$$

<u>Proof</u> $0 = 0 + 0 \Rightarrow a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$

Add $-(a \cdot 0)$ to both sides ($(R, +, 0)$ is a group!)

We get $0 = a \cdot 0$

Similarly $0 \cdot a = 0$ $\square$

<u>Corollary 21.2</u> Suppose R is a ring and $1 = 0$. Then $R = \{0\}$, the zero ring.

<u>Proof</u> $\forall a \in R$ $a = a \cdot 1 = a \cdot 0 = 0$.

From now on we'll tacitly assume that in a ring R, $1 \neq 0$.

<u>Definition</u> A field F is a commutative (nonzero) ring (so $1 \neq 0$) so that any nonzero element is a unit:

$\forall a \in F, a \neq 0$ $\exists b \in F$ s.t. $a \cdot b = 1 = b \cdot a$.

Ex $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. If p is prime $\mathbb{Z}_p$ is a field. $\mathbb{Z}$ is not a field. $\mathbb{Z}_n$ is not a field for n not prime.

Polynomial rings

Let R be a commutative ring. We "define"

$$R[x] = \{ a_0 + a_1 x + \cdots + a_n x^n \mid n \geq 0,\ a_i \in R \}$$

Note: if $m < n$

$$a_0 + a_1 x + \cdots + a_m x^m = a_0 + a_1 x + \quad + a_m x^m + 0 \cdot x^{m+1} + \cdots + 0 \cdot x^n$$

So we can define $+$ on $\mathbb{R}[x]$ by

$$\left(\sum_{i=0}^{n} a_i x^i \right) + \left(\sum_{i=0}^{n} b_i x^i \right) := \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{j=0}^{m} b_j x^j \right) := \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

We define $0 \in R[x]$ to be the zero polynomial 0

—— // — $1 \in R[x]$ to be the constant polynomial 1_R

Then $(R[x], +, \circ, 0, 1)$ is a commutative ring.

Definition The degree of $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ is

$$\deg p := \begin{cases} \max\{n \mid a_n \neq 0\} & \text{if } p(x) \neq 0 \\ -\infty & \text{if } p(x) = 0. \end{cases}$$

The reason for the convention that $\deg(0) = -\infty$ is

Lemma 21.3 For any two polynomials $f, g \in R[x]$
(R = a comm. ring)

$$(*) \quad \deg(f \cdot g) \leq \deg f + \deg g.$$

Proof If either f or g is 0, $f \cdot g = 0$ and $(*)$ says

$$-\infty \leq -\infty + \text{something finite}$$

Suppose next $f, g \neq 0$. Then $f(x) = a_0 + a_1 x + \dots + a_n x^n$ w
for some n, $a_1 \dots a_n \in R$, $a_n \neq 0$.
Similarly $g(x) = b_0 + \dots + b_m x^m$, $b_m \neq 0$.
And then
$$f(x)\, g(x) = a_n b_m x^{n+m} + \text{lower order terms.}$$
If $a_n b_m \neq 0$, $\deg(fg) = n+m = \deg f + \deg g$.
Otherwise $\deg(fg) < n+m = \deg f + \deg g$.

Ex $R = \mathbb{Z}_6$, $f(x) = [2]x^2$ $g(x) = [3]x^5 + [1]x$
Then $f(x)\, g(x) = [6]x^7 + [2]x^3 = [0]x^7 + [2]x^3$
So here $\deg fg = 3 < 2+5 = \deg f + \deg g$.

Rmrk You may be used to thinking of polynomials as functions
This is OK if $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ but not
in general

Rings of functions Let X be a set, R a ring
Let R^X = set of all functions from X to R.
R^X is a ring: $\forall f, g : X \to R$ we define
$$(f+g)(x) := f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x) \qquad \forall x \in X$$
The zero function $0(x) = 0_R$ $\forall x \in R$ is the zero of R^X
The constant function 1 defined by $1(x) = 1_R$ $\forall x \in X$
is the unity of R^X
and $(R^X, +, \cdot, 0, 1)$ is a ring.
<no proof>.

Note if $R = \mathbb{Z}_2$, $X = \mathbb{Z}_2$ $|R^X| = 2^2 = 4$
while $\mathbb{Z}_2[x]$ is infinite: $\forall n \geq 0$ $[1]x^n \in \mathbb{Z}_2[x]$.