Rings

Def A ring R is a set with two binary operations $+, \cdot$ s.t.

1) $(R,+)$ abelian grp $\begin{cases} a+(b+c)=(a+b)+c \\ \exists 0: a+0=a=0+a \\ \forall a\in R \exists -a\in R: a+(-a)=0=(-a)+a \\ ab=ba \end{cases}$
2) $(R,\cdot)$ monoid $\begin{cases} a(bc)=(ab)c \\ \exists 1: a1=a=1a \end{cases}$
3) $(a+b)c = ac+bc$, $a(b+c)=ab+ac$ } distributive laws.

R is commutative if furthermore $ab=ba$ $\forall a,b\in R$.

Note I will always assume R has a multiplicative identity element 1

Def A (ring) homomorphism $\varphi: R \to S$ is a function between rings such that

1) $\varphi(x+y) = \varphi(x)+\varphi(y)$
2) $\varphi(xy) = \varphi(x)\varphi(y)$
3) $\varphi(1_R) = 1_S$

Note 1) says φ is a group homomorphism $(R,+) \to (S,+)$.
Recall that $\varphi(0_R) = 0_S$ and $\varphi(-x) = -\varphi(x)$ are automatically true for groups.
However, for monoids we can't say this. 2)-3) express that φ is a monoid homomorphism $(R,\cdot) \to (S,\cdot)$.

Example. $\mathbb{Z}$ and $\mathbb{Z}_n$ are rings.

$\varphi: \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = [a]_n$
is a ring homomorphism.
Both $\mathbb{Z}$ and $\mathbb{Z}_n$ are commutative.

Example $\mathbb{R}[x] = \{$ polynomials in x with real coefficients $\}$ is a commutative ring (with usual operations).

In fact, if R is any ring, then
$R[x] = \left\{ \sum_{k=0}^{n} r_k x^k \;\middle|\; \begin{matrix} n \geq 0 \\ r_k \in R \end{matrix} \right\}$ becomes a ring, using operations:

$$\left(\sum_{k=0}^{n} r_k x^k\right) + \left(\sum_{l=0}^{m} s_l x^l\right) = \sum_{k=0}^{\max(n,m)} (r_k + s_k) x^k$$

(where we put $s_l = 0$ for $l > m$ and $r_k = 0$ for $k > n$) and

$$\left(\sum^{n} r_k x^k\right) \cdot \left(\sum^{m} s_l x^l\right) =$$

$$= \sum_{j=0}^{n+m} \left(\sum_{\substack{0 \le k \le n \\ 0 \le l \le m \\ k+l=j}} r_k s_l \right) x^j$$

Example. $M_n(R)$ $n \times n$-matrices with entries from a ring R (eg. $R = \mathbb{R}$ or $\mathbb{Z}$ etc)

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$

$$[a_{ij}] \cdot [b_{ij}] = \left[\sum_k a_{ik} b_{kj}\right]$$

$$1_{M_n(R)} = \begin{bmatrix} 1_R & & 0_R \\ & 1_R & \\ 0_R & & \ddots \\ & & & 1_R \end{bmatrix}$$

Example If A is an abelian group, then we get a ring:

$$\mathrm{End}(A) = \{\text{endomorphisms } \varphi : A \to A\}.$$

(An endomorphism is a group (or ring, monoid, etc) homomorphism from a group to itself)

$\varphi + \psi$ is defined by

$$(\varphi + \psi)(a) = \varphi(a) + \psi(a) \quad \forall a \in A.$$

$\varphi \cdot \psi = \varphi \circ \psi$ composition.

If A is replaced by a vector space V, and we require $\varphi : V \to V$ to be linear we get the ring

$$\mathrm{End}(V) = \{\text{linear maps } \varphi : V \to V\} = \mathcal{L}(V)$$

Def $r \in R$ is a **unit** if

$\exists\, r' \in R$ s.t. $rr' = 1_R = r'r$

In this case r' is unique and denoted r^{-1}.

Example. The ring of **real quaternions** is $\mathbb{H} = \{a1 + bi + cj + dk \mid a,b,c,d \in \mathbb{R}\}$.

As a vector space over $\mathbb{R}$, $\mathbb{H}$ is 4-dimensional. Addition is usual vector space $+$. Multiplication is linear in each argument and

$$ij = k = -ji \qquad i^2 = -1$$
$$jk = i = -kj \qquad j^2 = -1$$
$$ki = j = -ik \qquad k^2 = -1$$

So $(1+k)(2+i) = 2 + i + k(2+i) =$

$= 2 + i + 2k + ki = j$

$= 2 + i + j + 2k$

Note $ww^* =$

$= (a+bi+cj+dk)(a-bi-cj-dk) =$

$= a^2+b^2+c^2+d^2$

$+i(ab - ab + cd - cd)$

$+j(\ldots) \quad +k(\ldots)$

$= a^2+b^2+c^2+d^2 > 0 \quad$ if $w \neq 0$

Thus $w \cdot \frac{w^*}{ww^*} = 1$

Every nonzero element of $\mathbb{H}$ is a unit.

Def A ring R is a <u>division ring</u> if every nonzero element is a unit. A <u>field</u> is a commutative division ring.

Ex $\frac{\mathbb{R}[x]}{(p(x))}$ ring of congruence classes

$f(x) + (p(x)) = [f(x)]$, $f(x) \in \mathbb{R}[x]$

$[f(x)] = [g(x)] \iff p(x) \mid f(x) - g(x)$

$[f(x)] + [g(x)] = [f(x) + g(x)]$

$[f(x)] \cdot [g(x)] = [f(x)g(x)]$.

$a(x) \mid b(x) \iff \exists d(x) \in \mathbb{R}[x]$ $a(x)d(x) = b(x)$

Ex $R = \frac{\mathbb{R}[x]}{(x^2+1)}$

By division algorithm, any $f(x) \in \mathbb{R}[x]$ can be divided

$f(x) = (x^2+1)\underbrace{q(x)}_{\text{quotient}} + \underbrace{r(x)}_{\text{remainder, has deg} < 2 \text{ or } r(x) = 0}$

Note $[f(x)] = [r(x)]$.

So $R = \{ [a+bx] \mid a, b \in \mathbb{R} \}$

Can generalize to $\frac{\mathbb{F}[x]}{(p(x))}$, $\mathbb{F}$ any field.