Rings

$\mathbb{Z}$, ring of integers.

$\mathbb{Q}$, ring. (field)

$\mathbb{Z}/n\mathbb{Z}$.

Defn (ring). A ring R is a set with two binary operations, addition "$+$", multiplication "$\times$" such that

① With "$+$", R is a abelian group
identity element denoted by "0"
inverse of x is denoted by "$-x$"
$a+b = b+a$.
$(a+b)+c = a+(b+c)$
$a+0 = 0+a = a$
$a+(-a) = (-a)+a = 0$.

② "$\times$" is commutative. associative.
with identity element "1".

$a \times b$ $\quad ab$.

$ab = ba$, $\quad (ab)c = a(bc)$

$a \cdot 1 = 1 \cdot a = a$.

(3) Distributive law. $\quad a(b+c) = (b+c)a$

$= ab + ac$.

Commutative ring with "1"

↓

"×".

Ex: $(\mathbb{Z}, +, \times, 0, 1)$

$(\mathbb{Q}, +, \times, 0, 1)$

Ex: $R = \{0\}$.

Prop: If $1 = 0$, $R = \{0\}$. Pf: $1 \cdot a = a = 0$.

Prop: $0 \cdot a = 0$.

Pf: $0 + 0 = 0$. $\quad (0+0)a = 0a + 0 \cdot a$.

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

$$(-0\cdot a) + 0\cdot a = (0\cdot a + 0\cdot a) + (-0\cdot a)$$

$$0 = 0\cdot a.$$

Let $n \in \mathbb{Z}$, we can also view n as an element in R. by $n = \underbrace{1+1+\cdots+1}_{n}$

Then $a \in R$, $n\cdot a = (1+\cdots+1)\cdot a$

$$= \underbrace{a+a\cdots+a}_{n}.$$

Defn: (Unit) An element $a \in R$ is called a unit if a has multiplicative inverse b.

i.e. $\exists b \in R$, s.t. $ab = ba = 1$.

Inverse of a is unique, denoted by a^{-1}

Polynomial ring.

R ring, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

formal polynomial. $a_i \in R$.

x^i monomial.

$f(x) = a_n x^n + \cdots + a_0$

$g(x) = b_m x^m + \cdots + b_0$.

$f = g$ iff $m = n$, $a_i = b_i$.

Defn: $R[x] = \{$ formal polynomials with coefficients in R $\}$.

$f(x) = a_n x^n + \cdots + a_0$

$g(x) = b_m x^m + \cdots + b_0$.

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

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

Verify this is a ring.

$R[x, y] = R[x][y]$.

Division with remainder.

$g(x), f(x) \in R[x]$

If $g(x) = f(x)\cdot q(x) + r(x)$, $\deg r < \deg f$.

Divide $g(x)$ by $f(x)$ with remainder $r(x)$.

Prop (DWR): Division with remainder can be done if the leading coefficient of f is a unit.

In $\mathbb{Q}[x]$, $f(x) = 2x+1$, $g(x) = x^2+1$.

$$
\begin{array}{r|l}
2x+1 & \frac{1}{2}x - \frac{1}{4} \\
\cline{2-2}
x^2+1 & \\
x^2 + \frac{1}{2}x & \\
\hline
-\frac{1}{2}x + 1 & \\
-\frac{1}{2}x - \frac{1}{4} & \\
\hline
\frac{5}{4} &
\end{array}
$$

$$g(x) = \left(\frac{1}{2}x - \frac{1}{4}\right) f(x) + \frac{5}{4}.$$

In $\mathbb{Z}[x]$, $f(x) = 2x+1$, $g(x) = x^2+1$.

DWR cannot be done for $f(x), g(x)$ in $\mathbb{Z}[x]$.

If $(x^2+1) = (2x+1)\cdot q(x) + r(x)$,

$\deg r(x) < 1$.

leading term. (with highest degree in $q(x)$) must be $\frac{1}{2}x$.

Defn (Fields). $R \setminus \{0\}$ are all units.

$R \neq \{0\}$ $(0 \neq 1)$

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$. p prime $\neq$.

(Defn) subring. $R' \subset R$. subset

closed under $+, -, \times$.

$0, 1 \in R'$

Homomorphism between R_1 and R_2.

R_1, R_2 rings.

Defn: $f: R_1 \to R_2$. homomorphism

if ① f preserves "+", "×".

$\Leftarrow$ $f(a+b) = f(a) + f(b)$

$\begin{cases} f(1) = 0 \\ f(-a) = -f(a) \end{cases}$ $f(a \cdot b) = f(a) \cdot f(b)$.

② $f(1) = 1$

"$-a = (-1) \cdot a$."

Defn: (ker f) $\ker f = \{ a \in R_1 \mid f(a) = 0 \}$.

Prop: ① $\ker f$ is closed under addition.

"$-$". negation.

$0 \in \ker f$.

② If $s \in \ker f$, then $r \cdot s \in \ker f$ $\forall r \in R_1$.

Pf of ②: $f(rs) = f(r) \cdot f(s)$

$= f(r) \cdot 0 = 0$

$(0 \cdot a = 0)$.

Ex: $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$m \mapsto m \bmod n = \overline{m}$.

is ring homomorphism.

$\ker \pi = \{ nk \mid k \in \mathbb{Z} \}$.

$n > 1$ then $\ker \pi \neq 1$.

$\ker \pi$ is not a subring.

Prop: If $1 \in \ker f$, $1 \cdot a = a \in \ker f \ \forall a$.

$\ker f = R$

Ex: Evaluation map:

$R[x] \to R$. choose $s \in R$.

$p(x) \mapsto p(s)$

$$p(x) = a_n x^n + \cdots + a_0$$

$$p(s) = a_n \cdot s^n + \cdots a_0 .$$

$$s^n = \underbrace{s \cdot s \cdot \cdots s}_{n}$$

Prop (substitution principle)

$\varphi : R \to R'$ ring hom.

$\forall \alpha \in R'$, there exists a unique ring hom

$\underline{\varphi} : R[x] \to R'$, s.t. $\underline{\varphi}(x) = \alpha$.

$$\underline{\varphi}|_R = \varphi .$$

More generally, $\forall \alpha_1, \alpha_2 \cdots \alpha_n$

$\exists!$ $\underline{\varphi} : R[x_1, x_2 \cdots x_n) \to R'$.

s.t. $\underline{\varphi}(x_i) = \alpha_i$

$$\underline{\varphi}|_R = \varphi .$$

Pf: $p(x) = a_n x^n + \cdots + a_0$

$\underline{\varphi}(p(x)) = \varphi(a_n)\alpha^n + \cdots + \varphi(a_0)$

Defn (Isomorphism) Bijective homomorphism.

Ideal (very very important) $I \subset R$.

Defn: ① "additive" subgroup.

② $\forall s \in I$, $r \in R$, $s \cdot r \in I$.

Ex: $\ker f$ is an ideal

Defn: (Principal ideal) Fix $s \in R$.

$$sR = (s) = \{ sr \mid r \in R \}.$$

① closed under addition. "$-$".

$$r_1 s + r_2 s = (r_1 + r_2) s.$$

$$(-r) \cdot s = -(rs)$$

② $r' \cdot (rs) = (r' \cdot r) s$

More generally, ideal generated by $s_1, s_2 \dots s_n$.

$$(s_1, \dots s_n) = \left\{ \sum_{i=1}^{n} r_i s_i \mid r_i \in R \right\}.$$

Quotient ring:

Defn: $I \subset R$, ideal.

R/I = set of cosets under "+"

$= \{ a+I \mid a \in R \}$.

Defn and Thm: There exists a unique ring structure on R/I, s.t. $R \to R/I$ is

$a \mapsto a+I$.

a ring homo.

Pf: only need to define "×" on R/I.

$$(a+I)\cdot(b+I) \overset{\text{define}}{=} ab+I$$

"well-defined"?

$a_1+I = a_2+I$, want to check.
$b_1+I = b_2+I$. $a_1b_1+I = a_2b_2+I$.

depend on ② of defn of ideal.

First isomorphism Thm:

If $f: R \to R'$ surjective ring homo.

then $F: R/I \cong R'$. $I = \ker f$.

Pf depends on first iso Thm of groups.

① $F: (R/I, +) \cong (R', +)$.

② F preserves "$\times$".

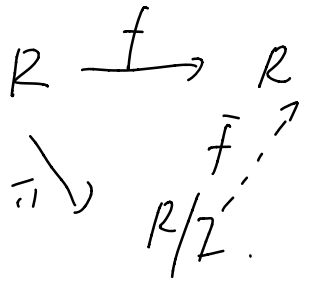
Mapping property:

If $f: R \to R'$ ring homo with

$\ker f = K$. $\pi: R \to R/I$.

a) If $I \subset K$, then $\exists!\ \bar{f}: R/I \to R'$.

s.t. $\bar{f} \cdot \pi = f$.



b) If $k=1$, then $\bar{f}: R/I \to R'$ is an isom.

Intuition: element in I are sent to zero in R/I.

"killing elements in I".

Ex: $\mathbb{Q}[x] \to \mathbb{Q}$. $\varphi(p(x)) = p(2)$.

$(x-2) \subseteq \ker\varphi$, because $\varphi(x-2) = 0$.

"1dim" $\Rightarrow$ $\ker\varphi = (x-2) = (x-2)\cdot\mathbb{Q}[x]$

principal ideal generated by $x-2$.