Concepts: ring, integral domain, field

ring: ① Abelian group under addition

② closed under multiplication, associative, distributive.

i) $0a+0\cdot a=(0+0)a=0\cdot a \Rightarrow 0\cdot a=0$

ii) $a(-b)=-(ab)$, $(-a)(-b)=ab$

unity = multiplicative identity → unique ($e_1\cdot e_2=e_1=e_2$)

unit: invertible element → unique ($bab'=e\cdot b'=be$)

"commutative": for multiplication

"$a|b$": $\exists c\in R,\ ac=b$

"$n\cdot a$" $(n\in\mathbb{N})$: $\underbrace{a+a+\cdots+a}_{n \text{ summands}}$

Subring & Subring test

Integral Domain: ① ring

② commutative

③ unity

④ no zero-divisors

$\Rightarrow$ law of cancellation

Field: ① integral domain (implies when finite)

② every non-zero element is invertible

↳ implies "no zero-divisors"

rmk: field is always integral domain.
for finite ring, integral domain is field.

characteristic $:= \min\{n \in \mathbb{N} \mid \forall x \in R\}$

$n=0$ if no such x.

prop: $0|1|_+ = \infty \Rightarrow n=0$

$|1|_+ < \infty \Rightarrow n = |1|_+$ (for ring with unity)

pf: $nx = n\cdot 1\cdot x = (n\cdot 1)\cdot x = 0\cdot x = 0$

② for integral domains

$n=0$ or prime

pf: $n\cdot 1 = (s\cdot t)\cdot 1 = (s\cdot 1)\cdot(t\cdot 1) = 0$
$\Rightarrow s\cdot 1$ or $t\cdot 1 = 0$

Ideal

ideal (two-sided): ① A is subring of R
② $\forall r \in R, a \in A, \Rightarrow ar \in A, ra \in A$.

rmk① very similar to 'normal subgroup'
② Note R_+ is Abelian $\Rightarrow$ every subgroup is normal
$\Rightarrow$ "only need to check $R_\times$" (it is ok to def R/A)

factor rings: R/A (defined iff A is ideal)

$(s+A)(t+A) := st + A$ (pf: $(s+s'+A)(t+t'+A) = st + s'A + At' + A^2 = st + A$)

$(s+A) + (t+A) := (s+t) + A$

For commutative ring only:

① prime ideal: i) proper ii) $ab \in A \Rightarrow a \in A$ or $b \in A$.

prop: R/A is integral domain iff A is prime

pf: integral domain $\Leftrightarrow$ $st + A = 0 + A \rightarrow$ $s+A$ or $t+A = 0+A$ $\Leftrightarrow$ $st \in A \rightarrow s \in A$ or $t \in A$ $\Leftrightarrow$ prime

② maximal ideal: i) proper ii) $A \subset B \subset R \Rightarrow B = A$ or $B = R$

prop: R/A is field iff A is maximal

pf: maximal $\Rightarrow \forall x \notin A$, $\langle x, A \rangle = R \ni 1$

$\Rightarrow \exists r \in R$, st. $xr + a = 1 \Rightarrow (x+A)(r+A) = 1+A$

$\Rightarrow x+A$ is invertible, R/A is a field

field $\Rightarrow \forall x+A$, $\exists y+A$, st. $xy = 1+a$

$\Rightarrow xy - a = 1 \in \langle x, A \rangle \Rightarrow \langle x, A \rangle = R \Rightarrow$ maximal

③ maximal implies prime.

for finite ring, prime = maximal.

(eg. $\langle x \rangle \subset \mathbb{Z}[x]$ is prime but $\subsetneq \langle x, 2 \rangle$, not maximal)

Illustration: assume $xy + a \in A$, A is maximal, $x, y \notin A$

1' x, y both invertible in $R \Rightarrow \underset{\in A}{x} = \underset{\in A}{a} y^{-1} \Rightarrow \times$

2' x not invertible $\Rightarrow xR \cup Rx \cup A$ is a bigger proper ideal $\Rightarrow \times$

3' y not invertible $\Rightarrow$ similarly $\times$

rmk: any irreversible x gives a proper ideal, namely xA

So $\forall xy \in A$, either $x \in A$ or $y \in A$.

Ring Homomorphism $\phi: R \to S$

def: preserve $+, \cdot$

prop: ① $\phi(1) = 1$ or 0 $\rightsquigarrow S \neq \{0\}$ (when ϕ is onto)

$\phi(0) = 0$

② preserve ideal in both directions ("$\Rightarrow$" requires ϕ be onto)

(requires "onto")

"$\Rightarrow$": $\forall x,\ xa \in A \Rightarrow \phi(x)\phi(a) \in \phi(A)$

"$\Leftarrow$": $a \in \phi^{-1}(B), \phi(a) \in B \Rightarrow \forall x,\ \phi(x)\phi(a) \in B \Rightarrow xa \in \phi^{-1}(B)$

③ preserve subring in both directions

"$\Rightarrow$" $a-b,\ ab \in A \Rightarrow \phi(a)-\phi(b),\ \phi(a)\phi(b) \in \phi(A)$

"$\Leftarrow$" $x, y \in \phi^{-1}(B),\ \phi(x), \phi(y) \in B \Rightarrow \phi(x-y), \phi(xy) \in B$

$\Rightarrow x-y,\ xy \in \phi^{-1}(B)$

④ i) $\ker\phi$ is ideal of R ii) $R/\ker\phi \cong \phi(R)$

iii) Ideals are all Kernels of some homomorphism.

iv) $R \to R/A,\ x \mapsto x+A$ is called natural homomorphism from R to R/A.

Z and ring with unity.

rmk: important trick — consider $\phi(1)$

thm: Let R be a ring with unity 1.

① $\Phi: \mathbb{Z} \to R$, $n \mapsto n \cdot 1$ is homomorphism

② $n \neq 0 \Rightarrow R$ contains $\mathbb{Z}_n$ (n is prime and R is field)

characteristic $n = 0 \Rightarrow R$ contains $\mathbb{Z}$ (+ R is field $\Rightarrow R$ contains $\mathbb{Q}$)

prime subfield: ① smallest and contain 1 ② contained in every subfield.

Field of Quotients

Def: For integral domain D,

$F = \{ \frac{a}{b} \mid a, b \in D \}$, with ① $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$,

② $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ ③ "=" $\Leftrightarrow ad = bc$, is field of quotients of D.

prop: ① is smallest field that contains D

② makes sense iff D is integral domain

i) $1 \in D \Rightarrow \frac{D}{1} \subset F$ ii) $b \neq 0, d \neq 0 \Rightarrow bd \neq 0 \Rightarrow \frac{ac}{bd}, \frac{ad+bc}{bd}$ is defined.

iii) $+, *$ being well-defined does not depend on integral domain property of D.

(well-defined → doesn't depend on representative of equivalence class)

Polynomial Rings

Application of division algorithm: (the algorithm works for $F[x]$ only when F is field)

① $f(a) = f(x) \bmod (x-a)$

② $F[x]$ is PID. polynomial with lowest degree is generator

rmk: remember to discuss the ideal $I=\{0\}$.

Reducibility & Factorization of polynomials

(rmk: D being integral domain $\Rightarrow D[x]$ being integral domain)

irreducible $f(x)$: ① $f(x)$ is not 0 or unit

② $f(x)=g(x)h(x) \Rightarrow g(x)$ or $h(x)$ is a unit

(this definition works for general integral domain (not only poly) as for integral domain, only need to consider g,h with degree $<$ deg f (cf. $g \in D[x]$))

Warning: for $\mathbb{Z}[x]$, numbers >1 should also be considered non-unit and implies reducibility

eg. $2x^2+4 = 2(x^2+2)$ is reducible over $\mathbb{Z}$

thm: for $f \in F[x]$, deg $f = 2$ or 3, reducible $\Leftrightarrow$ has zero

thm: $f \in \mathbb{Z}[x]$, reducibility over $\mathbb{Q}$ = reducibility over $\mathbb{Z}$

pf: Gauss's lemma (product of primitive poly is primitive)

content := gcd of coefficients = 1.

pf: Assume prime $p \mid$ new gcd and consider $\mathbb{Z}_p[x]$ as integral domain

thm: (mod p irreducibility) $f(x) \in \mathbb{Z}[x] \to \bar{f}(x) \in \mathbb{Z}_p[x]$, $\deg f = \deg \bar{f}$. then irreducibility of $\bar{f}/\mathbb{Z}_p$ implies that of $f/\mathbb{Q}$.

rmk: ① converse is not true

② may fail for all p

eg. x^4+1 is irreducible over $\mathbb{Q}$ but reducible over every $\mathbb{Z}_p$

thm. (Eisensteins) prime p s.t. $p \nmid a_n$, $p \mid a_i$ $(0 \le i \le n-1)$, $p^2 \nmid a_0 \Rightarrow f(x)$ is irreducible over $\mathbb{Q}$.

pf: consider $\sum_{i=0}^{n} a_i x^i = \left(\sum_{j=0}^{r} b_j x^j\right)\left(\sum_{k=0}^{s} c_k x^k\right)$

$a_0 = b_0 c_0 \Rightarrow p \mid b_0$ and $p \nmid c_0$ (without loss of generality)

$a_n = b_r c_s \Rightarrow p \nmid b_r \Rightarrow$ find ter s.t. $p \mid b_i$ $(i<t)$, $p \nmid b_t$

$\Rightarrow a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t$

($b_t c_0$: not divides p; $b_{t-1} c_1 + \cdots + b_0 c_t$: divides p; some terms here might be missing when $t > s$)

$\Rightarrow t = n$, $\deg c = s = 0$, contradiction.

Cor: p is prime $\Rightarrow \Phi_p(x) = \frac{x^p - 1}{x - 1}$ is irreducible over $\mathbb{Q}$

thm: in $F[x]$, $\langle p(x) \rangle$ be maximal $\iff p(x)$ is irreducible

pf: $F[x]$ is PID

thm: $F[x]$ is UFD (pf: PID implies UFD)

Divisibility (for Integral Domain)

Concept

① associates: $\exists$ unit u s.t. $a=bu$. then a "is an associate of b" or "a, b are associates" (is an equivalence relation)

② irreducible: ① $a\neq 0$, a is not unit,
② $a=bc \Rightarrow$ b or c is unit

③ prime: ① $a\neq 0$, a is not unit
② $a \mid bc \Rightarrow a\mid b$ or $a\mid c$.

rmk: ① a is prime $\Leftrightarrow \langle a\rangle$ is prime ideal
② in general, irreducibility $\not\Rightarrow$ prime
eg. in $Z[\sqrt{-3}]$, $1+\sqrt{-3}$ is irreducible but not prime
$N(1+\sqrt{-3})=4=2\times 2$. but N can't be $2 \Rightarrow$ irreducible
$(1+\sqrt{-3}) \nmid (2\times 2)$ as $(1+\sqrt{-3})(1-\sqrt{-3})=4 \Rightarrow$ not prime
③ prime $\Rightarrow$ irreducibility
$a=bc \Rightarrow a\mid b$ or $a\mid c$, say $a\mid b$
$\Rightarrow at=b \Rightarrow bct=b$, $ct=1 \Rightarrow c$ is unit

thm: PID $\Rightarrow$ irreducible equals prime

pf: $a\mid bc$, a is irreducible
Consider ideal $I=\{ax+by \mid x,y\in D\} \overset{\text{PID}}{=\!=} \langle d\rangle$
$\Rightarrow a=dt$ for some $t \Rightarrow$ d is unit (trivial) or t is unit ($(a\sim d)\mid b$)

$a\mid b$
$\uparrow$
$\langle d\rangle=\langle a\rangle$

$\mathbb{Z}[\sqrt{d}]$: a commonly used example.

$\mathbb{Z}[\sqrt{d}] := \{a+b\sqrt{d} \mid a,b\in\mathbb{Z}$ and $d\in\mathbb{Z}$, $\mu(|d|)\neq 0\}$

$N(a+b\sqrt{d}) := (a+b\sqrt{d})(\underbrace{a-b\sqrt{d}}_{\text{conj}(a+b\sqrt{d})}) = a^2-b^2\cdot d$

↳ called norm

prop²: ① $N(x)=0 \iff x=0$ ($a^2, b^2 \to$ square, $d \to$ not square $\Rightarrow a^2\neq b^2 d$ unless $a=b=0$)

② $N(xy)=N(x)N(y)$

sketch of pf: $(x+y\sqrt{d})(z+w\sqrt{d}) = (xz+wyd)+(xw+zy)\sqrt{d}$

$\Rightarrow \text{conj}(xy) = \text{conj}(x)\cdot\text{conj}(y)$

Cor: prime $N(x) \Rightarrow$ irreducible x over $\mathbb{Z}[\sqrt{d}]$

③ x is unit $\iff N(x)=1$ $(= x\cdot\text{conj}(x))$ with $x^{-1}=\text{conj}(x)$

Thm. PID implies UFD

A) lemma: in PID, "ideal tower" has finite height,

Pf: Suppose $I_1 \subsetneq I_2 \subsetneq I_3 \cdots$, $I = I_1 \cup I_2 \cup I_3 \cdots$ (union is ideal)

PID $= \langle a\rangle \Rightarrow a\in I \Rightarrow a\in I_n$ for some n. $\Rightarrow I=I_n$

Cor of lemma: every non-unit element has irreducible factor.

pf of cor: $a=a_0 \xrightarrow{b_1} a_1 \xrightarrow{b_2} a_2 \xrightarrow{b_3} a_3 \cdots$ until a_n is irreducible

Now consider Ideal Tower $\langle a_0\rangle \subsetneq \langle a_1\rangle \subsetneq \cdots$, this tower is finite $\Rightarrow$ the process must end eventually.

B) existence of irreducible factor implies existence of irreducible factorization.

c) "prime = irreducibility" implies uniqueness of factorization

pf: $a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$

$\Rightarrow p_1 \mid q_1 q_2 \cdots q_r$ (prime)

$\Rightarrow \forall i$ s.t. $p_1 \mid q_i \Rightarrow p_1 \cdot u = q_i$ (irreducible)

$\Rightarrow u$ is unit, $p_1 = q_i$ up to associates

cancel p_1, q_i and induct $\Rightarrow$ unique up to associates.

rmk: UFD $\not\Rightarrow$ PID

eg. $\mathbb{Z}[x]$ is UFD but not PID

moreover, D be UFD $\Rightarrow$ $D[x]$ be UFD

① "finite ideal tower" comes from "increasing degree"

any integral domain with this property is called "Noether domain"

existence of irreducible factorization

② unique factorization over $\mathbb{Q}$ + Gauss's lemma $\Rightarrow$ unique factorization over $\mathbb{Z}$

Euclidean Domain

Concept: for an integral domain D, it's ED if

$\exists\, d: D^{\neq 0} \to \mathbb{Z}_{\geq 0}$, s.t.

① $d(a) \leq d(ab)$

② $\forall\, a, b \in D,\ b \neq 0,\ \exists\, q, r$ s.t.

$a = qb + r$ and $(r = 0$ or $d(r) < d(b))$

Eg. $F[x]$ with $d(f) = \deg f$;

Gaussian integers with $d(a+bi) = a^2 + b^2$

Thm: ED implies PID.

pf: for ideal $I \neq \{0\}$, take out $a \in I$ s.t. $d(a)$ is smallest

$\forall\, b \in I$, assume $b = a \cdot q + r$

$r \neq 0 \Rightarrow d(r) < d(a)$, $r = b - aq \in I$, ×

$\Rightarrow r = 0 \Rightarrow a \mid b\ \forall\, b \in I \Rightarrow I = \langle a \rangle$.

For $I = \{0\}$, $I = \langle 0 \rangle$

rmk: PID $\not\Rightarrow$ ED. (though it's not easy to verify)