Chap 7: Rings

- Rings = Abelian gp ~~addition~~ + Assoc × + distributive laws
- comm rings if × is commutative. − Has identity if $\exists 1 \in R$, $1 \times r = r \times 1 = r$ $\forall r \in$
- Division ring/skew ring is a non-comm. field (every non-0 elem has an inv.)
- Non-comm rings: Ring of matrices & Hamilton Quaternions $\mathbb{H} = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{R}\}$
- Eg: rings of functions (additionally diff, cts, over $[0,1]$ etc)
- unit: $u \in R$ st. $\exists v \in R$, $uv = 1$. − R^* is the units of R, $F^* = F \setminus \{0\}$.
- Quadratic Integer Rings: $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is closed und. + and × when $D \equiv 1 \pmod 4$
  Consider the ~~rings~~ $\mathbb{Q}[\sqrt{D}]$, and the subrings
  quadratic field $= \{a+b\sqrt{D} \mid a,b \in \mathbb{Q}\}$ $\mathbb{Z}[\omega] = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \bmod 4 \end{cases}$
  $\mathbb{Q}$.
  $D \in \mathbb{Z}$. when $D=1$ we have the gaussian ints.
- subgroup $\xrightarrow[\text{unit}]{\text{closed und}}$ subring $\xrightarrow[rS \subseteq S]{\forall r \in R,}$ ideal. − finite ID is a field.
- Hom: Gp hom $\phi(a+b) = \phi(a) + \phi(b)$, Ring hom $\phi(a+rb) = \phi(a) + \phi(r)\phi(b)$.
  Module hom $\phi(a+rb) = \phi(a) + r\phi(b)$.
- Image of hom is a subring, kernel of hom is an ideal.
- Ideals $I+J = \{a+b \mid a \in I, b \in J\}$. $IJ = \{\sum_{\text{finite}} ab \mid a \in I, b \in J\}$.
  $IJ = I \cap J$ if $I+J = R$. Comaximal
- Comm ring is a field $\Leftrightarrow$ ideals are 0 and R
  $\Leftrightarrow$ every non-zero elem is a unit.
- Field $\Rightarrow$ homs from fields are injections or 0.
- every ideal is ~~prop~~ contained in a maximal ideal (if R has 1).
- R/M is field $\Leftrightarrow$ M is max R/P is ID $\Leftrightarrow$ P is ID.
  Commutative! and in comm Rings, maximal $\Rightarrow$ prime.

- Given Ring R, subset $D \subset R$ where ① no zero/divisors ② closed under mult in D.
  Then $\exists$ comm ring $Q (= D^{-1}R)$, where ① contains R as a subring.
  ② $\forall d \in D$, d is a unit in Q.
- If R is an ID then $D = R \setminus \{0\}$, we call Q the field of fractions/quotient field.
- CRT: $R/(A_1 A_2 \dots A_k) \cong R/(A_1 \cap A_2 \cap \dots \cap A_k) \cong R/A_1 \times R/A_2 \times \dots \times R/A_k$
  if $A_i + A_j = R$ whenever $i \neq j$. Proof: consider $R \to R/A_1 \times R/A_2$, and show kernel is
  $A_1 \cap A_2 = A_1 A_2$, and the map is surj.
  In particular, if $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$.
  units version: $(\quad)^* \cong (\quad)^* \times \dots \times (\quad)^*$.
  Since RHS is unit iff all coords are units.

Chap 8: Integral Domains

Commutative, $\text{Fields} \underset{\mathbb{Z}}{\subsetneq} \text{ED} \underset{\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]}{\subsetneq} \text{PID} \overset{\mathbb{Z}[x]}{\subsetneq} \text{UFD} \overset{\mathbb{Z}[\sqrt{5}i]}{\subsetneq} \text{ID}$.

— Defn: ED: Norm: $N: R \to \mathbb{Z}_{\geq 0}$.
tve norm: $N: R \to \mathbb{Z}_{>0}$.
: R is a ED if $\exists$ norm N, s.t. $\forall a, b \in R, b \neq 0, \exists q, r \in R$, s.t. $a = qb + r$ and $N(r) < N(b)$. or $r = 0$.

Eg: ① field F $\Leftrightarrow$ $F[x]$ is a ED with $N(p(x)) = \deg(p)$.

② Discrete valuation Ring: K field, discrete valuation $v: K^* \to \mathbb{Z}$ s.t.
(i) $v(ab) = v(a) + v(b)$.
(ii) v is surjective. (iii) $v(x+y) \geq \min(v(x), v(y))$ $\forall x, y \in K^*$ when $x + y \neq 0$.

The discrete valuation $v \cup \{(0,0)\}$ is a ~~norm~~ euclidean norm because
$N(a) < N(b) \Rightarrow a = 0 \cdot b + 0$.
$N(a) \geq N(b) \Rightarrow a = qb + 0$ where $q = ab^{-1}$; $v(q) = v(a) + v(b^{-1})$
Valuation ring $R = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}$. contains 1.

Facts: ① R is a subring of K. ② $v(1) = 0$ ③ $v(x) = -v(x^{-1})$ $\forall x \in K^*$.
④ x is a unit in R $\Leftrightarrow$ $v(x) = 0$.

③ ~~Conjugacy class~~ Center in a Gp Rt Ring: $Z(R) = \{x \in R \mid xa = ax \ \forall a \in R\}$
is a subring of R.

④ Center of a gp ring: $Z(R[G]) = \{\sum a_{C_i} (\sum_{g \in C_i} g) \in R[G] \mid a_{C_i} \in R, C_i \text{ are conjugacy classes of } G\}$.
over a finite gp G
R comm.

recall: Conj. classes of G is an orbit under LCA.

— Prop: ED $\Rightarrow$ PID.
Let any I in R (ED) be given. claim: The elem with minimal norm in I generates I: let it be d, $N(d) \leq N(r)$ $\forall r \in I$. ☆.
Claim: $(d) = I$. $(d) \subseteq I$ since $d \in I$.
$(d) \supseteq I$ since $\forall r \in I$, $r = qd + \text{rem}$ where $N(\text{rem}) < N(d)$ ~~and since N(d) is minimal~~ or rem=
$\text{rem} = 0 \Rightarrow r = qd \Rightarrow r \in (d)$.
$N(\text{rem}) < N(d) \Rightarrow$ $\text{rem} = r - qd$. but $r \in I, d \in I$.
$\text{rem} \in I$ and by minimality, $\text{rem} = 0$.

— Defn: $a \mid b$ if $\exists x \in R$, $ax = b$. gcd: $\forall d' \mid a, d' \mid b$, $d \mid a \wedge d \mid b \wedge d \mid d'$.

— Idea: finding the generator (principal) of a ED via the Euclidean Algorithm is based on reducing the norm. since $a - qb = r$, $r \in (a, b)$. but has smaller norm.
① If not PID, might not exist. ② might have multiple, differ by units.
③ If not ED, no norm.

Chap 9: Polynomial Ring.

R	R[x]
ID	ID
UFD	UFD
Field	~~PID~~/ED if norm = deg.

R	R[x]
Noetherian	Noetherian.

- $(R/I)[x] \cong R[x]/I[x]$.

  in particular, I prime in R $\Rightarrow$ I[x] prime in R[x].

  but max $\not\Rightarrow$ max.

- $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$.

  $n\mathbb{Z}[x]$ is prime if n=p. otherwise if n is composite, $\mathbb{Z}/n\mathbb{Z}[x]$ not ID.

- multivariable: $R[x_1, x_2] \cong (R[x_1])[x_2]$

  Defn: every polynomial in $R[x_1, \dots, x_n]$ $= \sum_{\text{finite}} r \underbrace{x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}}_{\text{monomial}}$.

  degree $= d_1 + d_2 + \dots + d_n$. multideg $= (d_1, \dots, d_n)$.

  a polynomial is homogenous if degree of all terms equal.

  homogenous comp of deg k = sum of all terms of deg k.

- deg n $\Rightarrow$ at most n roots $\forall p(x) \in F[x]$.

- $F[x]/(f(x))$ is ~~prime/irred/maximal~~ is field $\Leftrightarrow$ $(f(x))$ is maximal/prime/irred.

- if $p(x) \neq u\,q(x)$, then $(p^{a}(x)) + (q^{b}(x)) = F[x]$ comaximal.

- $F[x]/(f(x)) \cong F[x]/(p_1^{a_1}(x)) \times F[x]/(p_2^{a_2}(x)) \times \dots \times F[x]/(p_n^{a_n}(x))$ (By CRT, since comaximal)

- Irreducible elems in F[x]:

  ① p(x) has factor of deg = 1 $\Leftrightarrow$ $\exists$ root $\alpha \in F$.

  ② suppose R has field of fractions F. Then p(x) is reducible in F[x] $p(x) = a(x)b(x)$

  $\Rightarrow$ p(x) is reducible in R[x] $p(x) = a(x)b(x)$ where $a, b \in F$.

  ③ ~~Deg~~ deg(p(x)) = 2 or 3 is reducible.

  $\Leftrightarrow$ has a factor of deg 1 $\Leftrightarrow$ has a root in F.

  ④ If r/s (no common factor) is a root of p(x), then

  $r \mid a_0$ = constant, $s \mid a_n$ = leading coeff.

  In particular, if p(x) is monic, any root in $\mathbb{Q}$ must be integer dividing the const term.

  ⑤ Irreducibility test: if p(x) is irreducible in R/I [x], it is irreducible in R[x] (converse is false).

  ⑥ Eisenstein's criterion: $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$, R is ID.

  Then if $a_{n-1}, \dots, a_1 \in (P)$, $a_0 \notin (P^2)$, then irreducible in R[x].

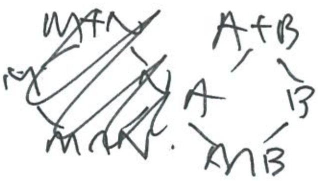
Chapter 10: Modules → ring on left/right resp.

- A left/right module over a ring R: M is an abelian gp wrt +, action $R \times M \to M$:

- $r \cdot (m+n) = r \cdot m + r \cdot n$	$(m+n) \cdot r = mr + nr$
- $rs \cdot m = r \cdot (s \cdot m)$.	$(m)(rs) = (mr)s$.
- $(r+s) \cdot m = r \cdot m + s \cdot m$.	$m(r+s) = mr + ms$.
- $1m = m$ if $1 \in R$.	$m \cdot 1 = 1$.

- Submod: an ab. subgp of M s.t. it is closed under action of R. $N \subset M$, $R \curvearrowright N \to N$
- Special submods: $\text{Ann}_R(M) = \{r \in R \mid r \cdot m = 0 \; \forall m \in M\}$. (not a submod)
  $\text{Tor}(M) = \{m \in M \mid r \cdot m = 0 \text{ for some } r \in R\}$
- $\mathbb{Z}$-mods: are abelian gps, if action is defined as ~~[illegible]~~ $(n, m) \longmapsto \underbrace{m+m+\ldots+m}_{n \text{ times}}$

  $\mathbb{Z}$-submods: are abelian subgps.
- $F[x]$ mods ~~where~~ are F-modules / F-vectorspaces by default, where x acts as a transformation $T: V \to V$
  $F[x]$ submods $\Longleftrightarrow$ F-vector spaces that are T-stable.
  $F[x]$ mods $\Longleftrightarrow$ F-vector spaces ~~that are~~ with $T: V \to V$ trans.
- submod criterion: a subset S of M is a submod if $\forall m, n \in S$, $r \in R$, $m + rn \in S$. $S \neq \emptyset$.
- Algebra $= (A, f: R \to A)$ s.t. $f(R) \subset Z(A)$. is a ring, where it is a natural left & right R-mod: $r \cdot a = a \cdot r = f(r) \cdot a$.
  ring ring
  eg: comm ring R: ① is a $\mathbb{Z}$-algebra. with the map $f(1_R) = (1_R)$.
  ② $R[x]$ is a R-algebra.
  (2.1) RG is a R-algebra.
  ③
- R-mod hom: $\phi(m + rn) = \phi(m) + r\phi(n)$.
- $\text{Hom}_R(M, M)$ is a ring with 1. $\text{End}_R(M)$ is a R-algebra if R is comm.
- Sum of mods: $A + B = \{a + b \mid \forall a \in A, b \in B\}$.
- Isom thm: M, N denote R-modules
  1. $\phi: M \to N$, $\phi \in \text{Hom}_R(M, N)$, then $M/\ker\phi = N$.
  2. A, B submod of M, Then $A+B/A \cong B/A \cap B$.
  3. Suppose $A \leq_m B \leq_m M$, $\therefore$ $M/A / B/A \cong M/B$.
  4. M/A: submods in M containing A $\Longleftrightarrow$ submods in M/A.



Chap 10.3: Generation, direct sum, free mods

Defn 1. sum $N_1+\dots+N_k=\{\sum_{\text{finite}} n_i . \mid i\in\{1,\dots,k\}.)$

2. R ring, A ~~submod~~ subset of M, then $RA=\{\sum_{\text{finite}} r_i a_i \mid r_i\in R, a_i\in A\}$.

3. Submodule $N\le M$ is f.gen. if $\exists$ subset $A\subseteq M$ finite, $RA=N$.

4. ~~Cyc~~ cyclic module if $A=\{a\}$.

Direct pt (direct sum) to sum: equiv

- $\pi: N_1\oplus\dots\oplus N_k \to N_1+\dots+N_k$ by just summing, is an isom. $\le M$.

$\iff N_j\cap(N_1+\dots+N_{j-1}+N_{j+1}+\dots+N_k)=0\ \forall j$.

$\iff$ Every $x\in N_1+\dots+N_k$ can be uniquely written in the form $a_1+\dots+a_k$, $a_i\in N_i$.

if satisfy above, then is direct sum.

- $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ is a direct sum since every element.

Free module: $F(A)$ can be written uniquely by $r_1a_1+r_2a_2+\dots+r_na_n$

- free modules over the same subset are isomorphic via identity.

~~M/p_1M~~ let $M = R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2)$.

$= R/(q_1^{b_1}) \oplus \dots \oplus R/(q_n^{b_n})$.

$$M/p_1M = \frac{R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2)}{p_1(R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2).)}.$$

let $F = R/(p_1)$. $= \cancel{\frac{R/(p_1)}{p_1 R/(p_1)} \oplus \cdots \frac{F}{p_1F}} \oplus F \oplus F \oplus 0$

$\cong$

a few words ① take distinct primes.

Result: $LHS = F^n \cong F^{n'} \Leftarrow$ grad.

② for a prime, try powers from 1 over until M/p^xM is 0.

Result: we must obtain $\overset{a_1 \longrightarrow b_1}{p_1 \quad = p_1}$

Noetherian Rings:

- A Ring is left noetherian if its left ideals fulfill ASC.
- Any module of left noetherian ring is Noetherian $\Longleftrightarrow$ any submod is fingen

  fingen. ~~&~~ a quotient of the free mod R^n which is noetherian. $\Longleftrightarrow$ any submod/quotient is noetherian.

- Any fingen mod over PID ($\Rightarrow$ Noeth) is finitely presented. ie,

  $M \cong \text{coker}(\varphi: R^m \to R^n)$.

- Mstraturnal Lemma: $\forall$ isom T, S, $\underset{R^m \to R^n}{\text{coker}(\varphi)} \cong \text{coker}(T\varphi S)$.
- Smith Normal Form: any φ as matrix can be ~~nn~~ transformed into $\text{diag}(d_1, d_2, \dots, d_n, 0, \dots, 0)$ where $d_1 | d_2$.
- $M \cong R/(d_1) \oplus R/(d_2) \oplus \dots \oplus R/(d_n) \oplus R^k$. $d_1|d_2|\dots|d_n$, $d_i \notin R^*$, $d_i \neq 0$.
- by Chinese Rem. Thm, $R/(d_1) \cong R/(p_1^{a_1}) \oplus \dots \oplus R/(p_k^{a_k})$.

  $\therefore M \cong R/(p_1^{a_1}) \oplus \dots \oplus R/(p_k^{a_k}) \oplus R^n$ not nec. distinct p_i.

- $\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some } r \in R\}$
- M is free $\Longleftrightarrow \text{Tor}(M) = 0$ (torsion free) for f.g. mod over PID
- Uniqueness: Free parts are equal since $R^k \cong \underset{\overset{\|}{R/(d_1) \oplus \dots \oplus R/(d_n)}}{M/\text{Tor}(M)} \cong R^{k'}$.

  claim: $R^k \cong R^{k'} \Longleftrightarrow k = k'$

  by considering $(R/I)^k \cong (R/I)^{k'} \Rightarrow k = k'$. (linear alg).

marato e calando

emphatic accented — getting softer; dying away

R	R[x]
ID	ID.
UFD	UFD.
F	PID/ED if norm=deg.

$R[x]/I \cong (R/I)[x]$.

Finite ab subgp of (F^*_{x}) ∀ fields F is cyclic. ~~whatt~~

Let $G \subset F^*$ be a subgp of a field F. Then G is cyclic. (be and finite)

~~Pf~~ G is a finite abelian gp. Structure theory gives that $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$ where $d_1|\dots|d_n$.

Smith normal form

① ~~End~~ $\mathrm{Hom}_R(R^m, R^n) \cong \mathrm{Mat}_{m\times n}(R)$.

② Any f.g. module M over R, a PID (hence left Noetherian) is Noetherian.
$\Rightarrow R^n$ is fin. gen (by $\{(1,1,1,\dots,1)\}$) and is Noetherian.

③ Any f.g. mod M over R, a PID is finitely presented, i.e,
$M \cong \mathrm{coker}(\varphi : R^m \to R^n)$.

$$\begin{tikzcd} R^m \arrow[r] \arrow[dr, two heads, "\varphi"'] & R^n \arrow[r, two heads, "f"] & M \\ & \ker f \arrow[u, hook] & \end{tikzcd}$$

∴ construct f and φ, then.

existence: by $M = R\{m_1, m_2, \dots, m_n\}$ finitely-gen.

(also f.g. since submod of Noetherian R^n).

$\therefore M \cong R^n/\ker f = R^n/\mathrm{Im}\,\varphi = \mathrm{coker}(\varphi : R^m \to R^n)$. ☐.

④ (Notational/cosmetic Lemma): isoms T, S, (correct dims) then
$\mathrm{coker}(\varphi : R^m \to R^n) \cong \mathrm{coker}(T\circ\varphi\circ S : R^m \to R^n$.

⑤ Exam tip: if we have
$ax+by=0$,
$cx+dy=0$
$ex+fy=0$.

(1) Module/Ab gp gen by x, y is R^2/relations
~~∴ Let $f: R^2 \to M$, $(1,0) \mapsto (a,b)$~~
~~$(0,1) \mapsto (c,d)$.~~
~~$f = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$~~

(2). Let $R^2 \to M$, $e_1 \mapsto x$
$e_2 \mapsto y$.

Let $R^3 \to R^2$, $e_1 \mapsto$ ~~(a, c, e)~~ (a,b)
(map to kernel) $e_2 \mapsto$ ~~(b, d, f)~~ $(c,d$
(e_1, e_2) spans $e_3 \mapsto (e,f)$.

⑥ Impt lemma: $\exists T, S$, $T\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} S = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$
where $\alpha | \beta$ (actually $\alpha = \gcd(a,b)$, $\alpha\beta = ab$).
$\Rightarrow \exists S, T$ s.t. $T\varphi S = \mathrm{diag}(\alpha_1, \alpha_2, \dots, \alpha_n, 0, \dots, 0)$.
where $\alpha_1 | \alpha_2 | \dots\dots$

- Torsion part: suppose $R/(p_1^{a_1}) \oplus \dots \oplus R/(p_k^{a_k}) \cong R/(q_1^{b_1}) \oplus \dots \oplus R/(q_1^{b_l}) \cong M$.

[illegible] strategy: consider M/p_iM $\forall p_i, q_i$.

Claim: let $M = R/(a)$. then $M/pM = \begin{cases} R/(p) & \text{if } p \mid (a). \\ 0 & \text{otherwise}. \end{cases}$

---

① Rings, Ideals ✓
② ED, PID, UFD, Noetherian, Artinian ✓
③ Polynomial rings over fields & irreducibility
④ Mod, Submod, homs, ~~Cyclic~~
⑤ Cyclic, Free, Noetherian
⑥ Structure theory - SNF, RCF, JCF ✓

RCF/JCF: Qn: given a matrix $M_{n\times n}(F)$ with entries in F, can we simplify it?

Qn': $F[x]$ is ED ($\Rightarrow$ PID). Then any $F[x]$-mods with x acting as a matrix has the structure.

Consider f.g. modules over pid

vs: fin. dim v.s. over $F([x])$ where x acts as T.

- $\lambda I - T : V \to V$ has kernel, called <u>eigenspace</u> over <u>e.v.</u> λ of T.

$\ker(\lambda I - T) \neq 0 \iff \det(\lambda I - T) \neq 0$.

$\det(\lambda I - T) = 0 \iff \lambda I - T$ is singular $\iff$

- $\det(xI - T) = c_T(x)$ is the <u>characteristic polynomial</u>.
- Impt Thm: $V \cong \operatorname{coker}(xI - T)$ as $F[x]$-mods. ✓

recall V is the f.d. mod of $F[x]$ where x acts as T.

- Now structure theory gives. $V \cong \operatorname{coker}(xI - T)$

$\cong \operatorname{coker}(A(xI-T)B)$ where A, B are invertible/isom.

- $\therefore V \cong F[x]/(f_1(x)) \oplus \dots \oplus$ By SNF. This is the RCF.
- Prop: - RCF is unique for T/V.
  - T is similar to RCF (recall).
  - T similar to $S \iff$ same RCF. (as similarity commutes)
- $\operatorname{Ann}_{F[x]}(V)$ is a submod of $V \overset{\text{def}}{=} F^n$ &

$= (p(x))$ be the min. poly.

- Defn: PID: every Ideal is principal. — PID ⇒ Noetherian. (Pf: any ascending chain, take the union, = (a), then $a \in I_n$ in the chain, stabs on
  - gcd exists and is unique up to unit multiplication
  - prime ⇔ maximal (⇐ is true ∀ comm rings)
  - prime ⇔ irreducible. (UFD). — $R[x]$ is PID (or ED) ⇔ R is a field.

UFD: every non-zero element has unique prime factorization up to perm & associates.

- gcd can take lowest common power. — $\mathbb{Z}$ is a UFD, hence we have Fundamental thm of arithmetic.

ID ⇐ UFD ⇐ PID ⇐ ED ⇐ Fields.
$\mathbb{Z}[\sqrt{5}i]$. $\mathbb{Z}[x]$ $\mathbb{Z}[\frac{1}{2}(1+\sqrt{19}i)]$ $\mathbb{Z}$

— Dedekind Hasse Norm: $N: R \to \mathbb{Z}_{\geq 0}$
where ① $N(a)=0 \Leftrightarrow a=0$
② $\forall a,b \in R$, $a \in (b)$ or $\exists x,y \in R$, $0 < N(ax-by) < N(b)$
(in Euclidean Norm, $x=1$).

— ∃ DH-Norm on R ⇔ R is PID.

Quadratic Integers / Gaussian integers.

① if α is irreducible in $\mathbb{Z}[i]$, then $N(\alpha) = p$ or p^2.
(since $\mathbb{Z}[i]$ is ED, any irred/prime $(\pi) \subseteq \mathbb{Z}[i]$, $(\pi) \cap \mathbb{Z} = (p)$ is prime in $\mathbb{Z}$)

② if $N(\alpha) = p^2$, $\alpha = \beta\gamma$, then $p^2 = N(\beta)N(\gamma)$ either β or γ is unit and the other $= p$, or $N(\beta) = N(\gamma) = p$.

③ case when $N(\alpha) = p$, $p \equiv 0, 1, 2$ or $3 \pmod 4$
0: impos. $4 | p$
1: ④ reducible.
2: $p = 2$
3: $a^2, b^2 \equiv 0, 1 \pmod 4$. α must be irred.

p is irreducible
⇔ $p = (a+bi)(a-bi) = a^2 + b^2$

④ $p \equiv 1 \pmod 4 \Leftrightarrow p | n^2+1$ for some integer n (⇔ $n^2+1=0$ has soln in $\mathbb{Z}/p\mathbb{Z}$).
& (Pf: $p \equiv 1 \pmod 4 \Rightarrow 4 | p-1 \Rightarrow \exists x, o(x) = 4$ in $(\mathbb{Z}/p\mathbb{Z})^\times \Rightarrow x^2 = -1 \pmod p$
$\Rightarrow x^2+1 \equiv 0 \pmod p$.)

⑤ Classification of irreducible elems in $\mathbb{Z}[i]$:
① $1 \pm i$ (norm = 2) $p \equiv 2 \pmod 4$.
② primes $p \in \mathbb{Z} \subset \mathbb{Z}[i]$ (norm $= p^2$) and $p \equiv 3 \pmod 4$.
③ ($p \equiv 1 \bmod 4$): $a \pm bi$ where $a^2+b^2 = p \equiv 1 \pmod 4$.
(factors irred because norm $= p$)
&

Cor of ④: $p \equiv 1 \pmod 4$
$\Rightarrow p | n^2+1 = (n-i)(n+i)$ but.
$p\gamma = (n-i) \Rightarrow \overline{p\gamma} = n+i = p\bar{\gamma}$
$\Rightarrow p | 2i$ →

Dummit & Foote 7.1

Eg of rings/fields:

- real/rational Hamilton Quaternions are non-comm division rings.
  elements: $a+bi+cj+dk$ where $a, b, c, d \in \mathbb{R}$ or $\mathbb{Q}$.
  addition: $a_1+b_1i+c_1j+d_1k + (a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+\ldots+(d_1+d_2)k$.
  mult: use dist. law on the terms, but
  $i^2=j^2=k^2=-1$, $ij=-ji=k$, $ik=-ki=-j$, $jk=-kj=i$
  ↑ clearly non-comm.
  inverse (since it is a div. ring). $(a+bi+cj+dk)^{-1} = \dfrac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$ ← like complex conj.
- ring of functions. If the codomain of functions is a ring, then by fixing the domain, the set of all functions $f: X \to \underset{\text{(ring)}}{A}$ is a ring by the normal $+, \times$ of functions.
  ~~Q~~ Q1: is it comm? Ans: if A is comm.
  Q2: what is the 0? Ans: the "zero" function: $x \mapsto 0_A$.
  Q3: is there a 1? Ans: if A has id, then it is $x \mapsto 1_A$.
  (iff. the other way by contradiction).
  Q4: when is it division? Ans: if A is div. (then given any fn, construct a pointwise inverse).

  Note: X can be as big or as small. $[0,1]$, $\mathbb{R}$ are typical egs.
  Note: a special case is cont/diff fns, which are closed under $+, \times$.
- zero divisors cannot be units and v.v.
  if a is a zero divisor and a unit, $ab=0$, $b\neq 0$ and $av=1$.
  then $b = 1b =$ $avb = 0$. →←.

  Qn: can it be neither? yes. all integers in $\mathbb{Z}$ are neither.
  (except for 1, -1 which are units).
- in $\mathbb{Z}/n\mathbb{Z}$, the units are such that $\gcd(a,n)=1$.
  Pf: (⇐) $ax+ny=1$ for $x, y \in \mathbb{Z}$.
  then $\bar{x}$ witnesses $\bar{a}$ being a unit.
  (⇒) let a be a unit, $\bar{a}\bar{b}=\bar{b}\bar{a}=1$ ∴ $ab \equiv 1 \pmod{n}$.
  ∴ $kn = ab-1$ ⇒ $ab-kn=1$
  ⇒ $\gcd(a,n)=1$.

D&F 7.1 Exercises.

1. $(1+(-1))(-1) = (-1) + (-1)\cdot(-1) = 0$. $\Rightarrow (-1)\cdot(-1) = 1$.

2. Since u is a unit, $\exists v \in R$ s.t. $uv = 1 = (-u)(-v)$ $\Rightarrow -u$ is a unit.

3. Clearly it's true, since $\exists v \in S \subseteq R$.