

Last lecture

- An ideal is finitely generated if it is the sum of a finite number of principal ideals.
- If all of the ideals of R are finitely generated then R satisfies the ascending chain condition on ideals (Theorem 14.2).
- a is **irreducible** if $a \neq 0$, a is not a unit and $r|a$ only if r is either a unit or an associate of a .
- p is **prime** if $p \neq 0$, p is not a unit and if $p|bc$ then either $p|b$ or $p|c$.
- If R is an integral domain then every prime is irreducible (Lemma 14.6).
- If R is a PID and $0 \neq a \in R$ then a is prime if and only if R/aR is an integral domain.
- In general, irreducible does not imply prime!

This lecture

Unique factorization domains and PID \implies UFD.

Unique factorization domains

Definition 15.1

A **unique factorization domain** (UFD) is an integral domain R such that

- UF1 Every non-zero element of R can be written in the form $ua_1 \dots a_k$, where u is a unit, $k \geq 0$ and a_1, \dots, a_k are irreducible in R .
- UF2 If $ua_1 \dots a_k = vb_1 \dots b_l$, where u and v are units, $k, l \geq 0$ and $a_1, \dots, a_k, b_1, \dots, b_l$ are all irreducible then $k = l$ and, after renumbering if necessary, a_i and b_i are associates for $i = 1, \dots, k$.

This is the best that we can expect for uniqueness of factorization in a general commutative ring.

Examples

- Any field is a UFD since every non-zero element is a unit.
- By the prime factorization theorem, \mathbb{Z} is a UFD.
- By the last slide, the ring $\mathbb{Z}[\sqrt{-5}]$ is **not** a UFD.

We will see that every PID is a UFD.

Irreducibles and primes in a UFD

Proposition 15.2 (Prime = irreducible in a UFD)

Suppose that R is a unique factorization domain and that $0 \neq a \in R$ is not a unit. Then a is irreducible if and only if a is prime.

Proof Suppose that a is irreducible and that $a|bc$.

We must show that either $a|b$ or $a|c$.

Write $b = ub_1 \dots b_k$ and $c = vc_1 \dots c_l$, for units u and v and irreducible elements $b_1, \dots, b_k, c_1, \dots, c_l$ in R .

$$\implies bc = uvb_1 \dots b_k c_1 \dots c_l = ad, \text{ for some } d.$$

$$\implies uvb_1 \dots b_k c_1 \dots c_l = wad_1 \dots d_m, \text{ if } d = wd_1 \dots d_m, \\ \text{for } w \text{ a unit and } d_1, \dots, d_m \text{ irreducible}$$

$$\implies \text{either } a \sim b_i, \text{ for some } i, \text{ or } a \sim c_j, \text{ for some } j, \text{ by UF2.}$$

$$\implies a|b \text{ or } a|c \implies a \text{ is prime in } R$$

Conversely, suppose that a is prime and write $a = ua_1 \dots a_k$ as in UF1

$$\implies a|u (\implies a \text{ is a unit } \implies \text{not possible!}) \text{ or } a|a_1 \text{ or } \dots \text{ or } a|a_k.$$

$$\implies a \text{ and } a_i \text{ are associates for some } i \implies a = ua_1 \text{ is irreducible } \square$$

Factorization in a PID

Proposition 15.3 (UF1 for PIDs)

Suppose that R is a PID and that a is a non-zero element of R . Then $a = ua_1 \dots a_k$, where u is a unit and a_1, \dots, a_k are irreducible.

Proof If the only divisors of a are units and associates of a then a is already in the form of UF1 and there is nothing to prove.

Suppose that $a = xy$, where x and y are not units or associates of a . If x and y can both be written the form of UF1 then we are done.

By way of contradiction, suppose that x cannot be written in this form.

Set $a_1 = a$ and $a_2 = x$ then $a_2|a_1$ and a_1 and a_2 are not associates.

Repeating this argument with a_2 produces an element a_3 such that $a_3|a_2$ and a_2 and a_3 are not associates.

Continuing this way we can find elements a_1, a_2, a_3, \dots such that $a_{i+1}|a_i$ and a_i and a_{i+1} are not associates for $i \geq 1$.

This contradicts Corollary 14.4, and hence completes the proof. \square

[Choosing $a_{i+1}|a_i$ with $a_{i+1} \not\sim a_i$ requires the **Axiom of Choice!**]

PIDs are UFDs

Lemma 15.4

Suppose that R is a PID and that $a|bc$, and $\gcd(a, b) = 1$, for some $a, b, c \in R$. Then $a|c$.

Proof As $\gcd(a, b) = 1 \implies aR + bR = 1 \cdot R = R$ by Lemma 12.7.
 $\implies 1 = ar + bs$, for some $r, s \in R$
 $\implies c = c \cdot 1 = car + cbs \implies a|c$ since $a|a(cr)$ and $a|b(cs)$. \square

Corollary 15.5

Suppose that R is a PID. Then every irreducible element of R is prime.

Proof Suppose that $a \in R$ is irreducible and that $a|bc$.
Let $d = \gcd(a, b) \implies aR + bR = dR$ by Lemma 12.7 $\implies d|a$
 \implies either d is a unit or an associate of a since a is irreducible.
If d is a unit then $dR = R \implies 1 = \gcd(a, b)$ by Lemma 12.7
 $\implies a|c$ by Lemma 15.4
If a and d are associates then $dR = aR \implies a = \gcd(a, b) \implies a|b$.
Hence, p is prime in R as required.

PIDs are UFDs.../2

Corollary 15.6

Suppose that R is a PID, that $a \in R$ is irreducible and that $a|b_1 \dots b_l$. Then $a|b_i$, for some i .

Theorem 15.7 (PID \implies UFD)

Every principal ideal domain is a unique factorization domain.

Proof By Proposition 15.3 we only have to show that UF2 holds in R .
Suppose that $ua_1 \dots a_k = b_1 \dots b_l$, where $k, l \geq 0$, u is a unit and $a_1, \dots, a_k, b_1, \dots, b_l$ are irreducible.
We show by induction on k that $k = l$ and $a_i \sim b_i$, for all i .
If $k = 0$ then $u = b_1 \dots b_l \implies l = 0$. Similarly, $l = 0 \implies k = 0$.
Suppose then that $k, l \geq 1 \implies a_k | ua_1 \dots a_k = b_1 \dots b_l$
 $\implies a_k | b_i$ for some i by Corollary 15.6
 $\implies a_k$ and b_i are associates, for some i , since b_i is irreducible

PIDs are UFDs.../3

By renumbering if necessary, assume that a_k and b_l are associates.

$\implies a_k = vb_l$ for some unit $v \in R$
 $\implies b_1 \dots b_l = ua_1 \dots a_{k-1} a_k = uv a_1 \dots a_{k-1} b_l$
 $\implies b_1 \dots b_{l-1} = uva_1 \dots a_{k-1}$ as R is an integral domain
Now, uv is a unit so by induction $k-1 = l-1$ and $a_i \sim b_i$, for $i < k$.
 $\implies k = l$ and $a_i \sim b_i$ for $i = 1, \dots, k$ after renumbering, if necessary.

Hence, the factorization $ua_1 \dots a_k = b_1 \dots b_l$ is unique up to multiplication by units and taking associates, so that R is a UFD. \square

Corollary 15.8

The rings \mathbb{Z} , $\mathbb{Z}[i]$ and $F[x]$, for F a field, are UFDs.

Corollary 15.9

If R is a PID and $a \in R$ then a is irreducible $\iff a$ is prime.

Proof Immediate from Theorem 15.7 and Proposition 15.2 (or from Lemma 14.6 and Corollary 15.5). \square