21-237: Math Studies Algebra I November 14, 2022

Lecture 29 : PIDs are UFDs

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Principal ideals and association

Fact: Let R be ID, $a, b \in R$. The following are equivalent:

(1) $(a) = (b)$

(2) a, b are associates.

Proof: (2) $\implies$ (1). If a, b are associates, say $a = ub$ for unit u. Then also $b = u^{-1}a$. $a \in (b)$, so $(a) \subseteq (b)$ and $b \in (a)$, so $(b) \subseteq (a)$. Then $(a) = (b)$.

(1) $\implies$ (2). If $(a) = (b) = (0)$, then $a = b = 0$.

If $(a) = (b)$ non-zero, then $0 \neq a \in (b)$ and $0 \neq b \in (a)$, so $a = rb$ and $b = sa$ for $r, s \in R$, so $a = rsa$ and $0 = a(1 - rs)$.

We're in an ID, and $a \neq 0$, so $1 - rs = 0$, i.e. $rs = 1$. Thus, r, s are inverse units and a, b are associates. □

Similarly, **Fact**: The following are equivalent:

(1) $(a) \subseteq (b)$

(2) b divides a.

Easy fact: If R ID, $a \in R$, a is a prime element iff (a) is a non-zero prime ideal.

2 Properties of principal ideal domains

Let R be a PID.

Claim 1: $r \in R$ is irreducible iff (r) is a non-zero maximal ideal.

Proof: Exercise. □

Claim 2: If $r \in R$ is irreducible, then r is prime.

Proof: Maximal ideals are prime. Then apply Claim 1 and the easy fact. □

Summary: If R PID, then

(1) Prime ideals are 0 and (r) for r prime/irreducible.

(2) Maximal ideals are (r) for r prime/irreducible, or (0) if R field.

3 Sufficient conditions for being UFD

Theorem: If R ID, R Noetherian, and the prime and irreducible elements of R coincide, then R is a UFD. In particular, R PID $\implies$ R UFD.

Proof: **Part 1**, existence of factorizations. We show that if r is non-zero non-unit, then r is a finite product of irreducibles.

Note: r is finite product of irreducibles $\iff$ some associate is $\iff$ every associate is.

Suppose for contradiction that there is r nonzero, nonunit, not finite product of irreducibles. Let $X = \{(r) : r \text{ nonzero, nonunit, not product of irreducibles}\}$. $X \neq \emptyset$ by our hypothesis. As R is N'ian, X has an element (r) which is maximal under inclusion.

As $(r) \in X$, r is not irreducible. So $r = st$, where s, t are neither units nor associates of r. Also $s, t \neq 0$.

So (r) is strictly contained in (s) and (t). So $(s), (t) \notin X$ since (r) is maximal in X. So each of s and t is a finite product of irreducibles. As $r = st$, r is a finite product of irreducibles, a contradiction.

And now, for something completely trivial. If R ID and r_0, r_1 irreducible in R, then r_0 divides r_1 iff r_0, r_1 are associates.

Part 2, uniqueness of factorizations. Let $r \in R$, r nonzero nonunit, let $r = a_1 \dots a_s = b_1 \dots b_t$, a_i's b_j's irreducible.

Claim: $s = t$, there is $\pi \in S_t$ such that $a_i, b_{\pi(i)}$ are associates for all i.

Proof: a_1 is irreducible, so a_1 is prime. Also $a_1 \mid r = b_1 \dots b_t$, so there is j such that $a_1 \mid b_j$. From the trivial fact above, a_1, b_j are associates, say $a_1 = ub_j$. Then, $u \prod_{i \neq 1} a_i = \prod_{k \neq j} b_k$[1]. Cutting corners, $s - 1 = t - 1$, so $s = t$ and $ua_2 \dots a_s$ and $b_1 \dots b_{j-1} b_{j+1} \dots b_t$ are equal up to permutation and associates.

Note: If u unit, $u = xy$, x, y both units, and a unit is not a finite (non-empty) product of irreducibles. □

[1]We omit the reason that we can "divide by b_j," but this is an easy application of cancellation in IDs.