21-237: Math Studies Algebra I November 16, 2022

Lecture 30 : More on factorization and divisibility

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Greatest common divisors

Recall: PID $\implies$ UFD. Soon, we will show that the converse is not true, as $\mathbb{Z}[x]$ UFD but not PID.

Let R be an ID, $a, b \in R$. d is a **greatest common divisor** (gcd) of a, b if and only if

(1) d divides both a and b

(2) If e divides both a and b, then e divides a.

Note that from this definition, 0 is the only gcd of $0, 0$.

Further note that if d', a', b' are associates of d, a, b, then d is a gcd of a, b iff d' is a gcd of a', b'.

Facts:

(1) If a, b have a gcd, it's unique up to associates.

Proof: If d_1, d_2 are both gcd's, $d_1 \mid d_2$ and $d_2 \mid d_1$, so d_1, d_2 are associates. $\square$

(2) In a UFD, gcd's exist for all a, b.

Proof sketch: Compare factorizations of a, b. $\square$

(3) In a PID, $(a, b) = (d)$ for any gcd d of a, b.

Proof: $a \in (a, b) = (d)$, so $d \mid a$. Similarly, $d \mid b$.

If $e \mid a, b$, then $(e) \supseteq (a, b) = (d)$, so $e \mid d$. $\square$

2 Non-unique factorization domains

Recall: For $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, $|z|^2 = z\overline{z} = a^2 + b^2$. $|zw| = |z||w|$.

Let $\alpha = i\sqrt{5}$, let $R = \mathbb{Z}[\alpha] = \{m + n\alpha : m, n \in \mathbb{Z}\}$.

If $r = m + n\alpha \in R$, $N(r) = |r|^2 = (m + n\alpha)(m - n\alpha) = m^2 + 5n^2$.

Easy: $N(r) = 0 \iff r = 0$. Also, $N(rs) = N(r)N(s)$.

If $rs = 1$, then $N(r)N(s) = N(rs) = N(1) = 1$, so $N(r) = N(s) = 1$. So ± 1 are the only units.

Furthermore, R is an ID as R is a subring of a field.

Useful fact: $m^2 + 5n^2 \equiv 0, 1, 4 \bmod 5$ for integers m, n.

Claim: 2 is irreducible. *Proof*: If $2 = ab$, $4 = N(2) = N(a)N(b)$. From the useful fact, there are no elements of norm 2, so WLOG suppose $N(a) = 1$ and $N(b) = 4$. Then, a is a unit, so we're done. $\square$

Note: $N(1 + \alpha) = N(1 - \alpha) = 1^2 + 5 \cdot 1^2 = 6$.

Claim: 3, $1 - \alpha$, $1 + \alpha$ all irreducible. *Proof*: similar. $\square$

Note: $6 = 2 \times 3 = (1 + \alpha)(1 - \alpha)$, so R is not a UFD and $2, 3, 1 + \alpha, 1 - \alpha$ are not prime, even though they are irreducible.

Claim: There is no gcd of $6, 2(1+\alpha)$ in $\mathbb{Z}[\alpha]$. *Proof*: $2, 1+\alpha \mid 6, 2(1+\alpha)$. If d gcd, then $2 \mid d$ and $1+\alpha \mid d$, so $N(2) = 4 \mid N(d)$, $N(1+\alpha) = 6 \mid N(d)$, and $d \mid 6, 2(1+\alpha)$, so $N(d) \mid 36, 24$. Thus, $N(d) = 12 \equiv 2 \bmod 5$, a contradiction. $\square$

3 Linear algebra redux

Let M be an R-module.

(1) For $X \subseteq M$, $\mathrm{span}(X) =$ least submodule of M containing X.

(2) A set $Y \subseteq M$ is **independent** if for all distinct $y_1, \ldots, y_t \in Y$ and all $r_i \in R$, $\sum_{i=1}^{t} r_i y_i = 0 \iff$ all r_i's 0.

A **basis** for M is an independent spanning set. M is **free** if and only if M has a basis.