Lecture 19: Non PIDs; primes, irreducibles, and factorization.

§27-30 of [R2]
§8.2-8.3 of [DF]

Previously:

Euclidean Domain $\Rightarrow$ Principal ideal domain $\Rightarrow$ All prime ideals are maximal

Principal ideal domain $\Rightarrow$ gcd's exist.

Principal ideal domain $\Rightarrow$ (to do) Unique factorization

---

Non-PIDs:

① $\mathbb{Z}[x] \supseteq (2, x)$ Also $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$

$\Rightarrow (x)$ is prime but not max.

② $\mathbb{Q}[x,y] \supseteq (x,y)$ Also $\mathbb{Q}[x,y]/(y) \cong \mathbb{Q}[x]$

③ $R = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$.

Claim: $\alpha = 6$ and $\beta = 2+2\sqrt{-5}$ have no gcd.

Consider $N(a+b\sqrt{-5}) := |a+b\sqrt{-5}|^2 = a^2+b^2 5$,
so $N(\alpha) = 36 = 2^2 3^2$ and $N(\beta) = 24 = 2^3 \cdot 3$.
Suppose $\gamma = \gcd(\alpha,\beta)$. Then $\gamma \mid \alpha \Rightarrow N(\gamma) \mid N(\alpha)$
and $\gamma \mid \beta \Rightarrow N(\gamma) \mid N(\beta) \Rightarrow N(\gamma) \mid 12$. If η
is any common divisor of α, β, then $\eta \mid \gamma$
and so $N(\eta) \mid N(\gamma)$.

As 2 and $1+\sqrt{-5}$ are common divisors of (α, β) (as $6 = (1+\sqrt{-5})(1-\sqrt{-5})$) with norms 4 and 6, we learn $N(\gamma) = 12$. Now $2 \mid \gamma$, so $\gamma = 2\varepsilon$. Taking norms gives $N(\varepsilon) = 3$. But R has no elts of norm 3, a contradiction. $\blacksquare$

R integral domain, $r \in R$ nonzero and not a unit.

<u>reducible</u>: $r = a \cdot b$ with a, b nonunits.

<u>irreducible</u>: $r = a \cdot b \Rightarrow$ one of a, b is a unit.

<u>prime</u>: $r \mid ab \Rightarrow r \mid a$ or $r \mid b$.

<u>Note</u>: $r \in R$ is prime $\Leftrightarrow (r)$ is a prime ideal.

<u>Pf</u>: $r \mid s \Leftrightarrow s = qr \Leftrightarrow s \in (r)$. So the two statements are really the same. $\blacksquare$

<u>Thm</u>: A prime r is irreducible.

<u>Pf</u>: If $r = a \cdot b$, can assume $r \mid a$, i.e. $a = cr$.

Then $r = (cr)b = (bc)r \Rightarrow bc = 1 \Rightarrow b$ a unit.

$\blacksquare$

Ex: In $\mathbb{Z}[\sqrt{-5}]$, 3 is irreducible since $N(3) = 9 = 3^2$

and (a) only elts of norm 1 are ± 1;

(b) no elts of norm 3

$N(a+b\sqrt{-5}) = a^2 + b^2 5.$

However 3 is not prime as $3 \mid 9$ and

$9 = (2+\sqrt{-5})(2-\sqrt{-5})$ but $3 \nmid (2 \pm \sqrt{-5})$

as both have norm 9 but don't differ by ± 1.

Thm: In a PID, r irreducible $\iff$ r prime

Pf: ($\Rightarrow$) Will show (r) is maximal $\Rightarrow$ (r) prime $\Rightarrow$ r prime. Suppose $(r) \subseteq (a)$, so that $r = ab$. As r irred, either a is a unit $\Rightarrow (a) = R$

or b is a unit $\Rightarrow (a) = (r)$.

So (r) is maximal as needed. $\boxtimes$

R integral domain. Elts r, s are associates when $r = us$ for some unit $u \in R$.

<u>Unique Factorization Domain</u>: An int. domain where for every non-zero non-unit r have:

(a) $r = p_1 p_2 \cdots p_n$ where the p_i are irred.

(b) This is unique in that any other factorization $r = q_1 q_2 \cdots q_m$ has $n = m$ and can be reordered so that each q_i is an assoc of p_i.

<u>Ex</u>: PIDs [Next time]

because of norm.

<u>Non-Ex</u>: (1) $\mathbb{Z}[\sqrt{-5}]$ has (a) but not (b) since

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

(2) $\mathbb{Z}[\sqrt[n]{2} ; n \in \mathbb{Z}_{>0}]$ doesn't have (b) as

$2 = \sqrt{2} \cdot \sqrt{2} = (\sqrt[4]{2})^4 = (\sqrt[8]{2})^8 = \cdots$

<u>Basic props of UFDs</u>:

(1) Irreducible elts are prime

(2) gcd's exist. If $a = u p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $b = u' p_1^{e_1'} p_2^{e_2'} \cdots p_n^{e_n'}$ where p_i are non-assoc. irred, u and u' are units, then

$$\gcd(a,b) = \prod p_i^{\min(e_i, e_i')}$$

Pf: [Skip! Refer to notes or § 8.3 of [DF]]

(1) Suppose an irred r divides ab, so $ab = cr$

Expand a, b, c as prod of irred:

$(a_1 \cdots a_j)(b_1 \cdots b_k) = (c_1 \cdots c_\ell) \cdot r$

By uniqueness, some a_i or b_i is an assoc of r

$\Rightarrow r \mid a$ or $r \mid b$. ▨

(2) Set $g = \prod p_i^{\min(e_i, e_i')}$. Clearly $g \mid a$ and $g \mid b$. If d is any common divisor with $d = q^e r$ where q is irred, then $a = (q^e r) s$ and $b = (q^e r) \cdot s'$. Since rs and rs' have factorizations, uniqueness means q is an assoc of some p_i with $e \leq \min(e_i, e_i')$. So $d \mid g$ as needed. ▨