Announcements

Midterm exams will (very likely) be moved to

Wednesdays 7:00-8:30 pm

Need to book rooms; I'll let you know when this is confirmed

One last result about PIDs:

Prop: $R[x]$: PID $\Leftrightarrow$ R: field

Pf: $\Leftarrow$) If R: field, $R[x]$ is Euclidean (lecture 2) hence a PID.

$\Rightarrow$) $R[x]$ integral domain $\Rightarrow$ R integral domain

$\Rightarrow (x)$ prime (since $R[x]/(x) \cong R$)

$\Rightarrow (x)$ maximal (since it is a prime ideal in a PID)

$\Rightarrow R \cong R[x]/(x)$ field $\square$

Unique factorization domains

Recall/def: R integral domain, $r \in R$, $r \neq 0$, nonunit

- Irreducible: $r = ab \Rightarrow a$ or b is a unit
- Prime: $r \mid ab \Rightarrow r \mid a$ or $r \mid b$

(prime $\Rightarrow$ irred.)

- r and s are <u>associates</u> if $r \mid s$ and $s \mid r$ (i.e. if $r = us$, u: unit)

Goal for today/Friday: use factorization in $\mathbb{Z}[i]$ to prove

Thm (Fermat): Let $p \in \mathbb{Z}$ be prime. Then p is the sum of two squares: $p = a^2 + b^2$, $a, b \in \mathbb{Z}$ iff $p = 2$ or $p \equiv 1 \bmod 4$. This expression is unique up to order & sign.

Def: An integral domain R is a unique factorization domain if $\forall$ nonzero nonunit $r \in R$,

a) $r = p_1 \cdots p_n$ w/ $p_i \in R$ irred.

b) If also $r = q_1 \cdots q_m$ w/ q_i irred., then $m = n$ and there is some permutation σ of $1, \dots, n$ s.t. p_i is an assoc. of $q_{\sigma(i)}$

Soon: PID $\Rightarrow$ UFD

Prop: Let R: UFD, $r, s \in R$

a) r irred. $\Rightarrow$ r prime

b) If $r = u p_1^{e_1} \cdots p_n^{e_n}$, $s = v p_1^{f_1} \cdots p_n^{f_n}$ where u, v: units and p_i irreds. which are pairwise non-associates, then

$$d := p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$$

is a gcd of r and s.

Pf: a) Let r: irred. and suppose $r | ab$ i.e. $ab = cr$. Expand both sides as prods. of irreducibles:

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

and since R is a UFD, some a_i or b_i is an assoc. of r, so $r | a$ or $r | b$.

b) $d | r$ since

$$r = d u p_1^{e_1 - \min(e_1, f_1)} \cdots p_n^{\overbrace{e_n - \min(e_n, f_n)}^{\geq 0}},$$

and similarly $d | s$. Let c be any common divisor of r and s, w/ irred. factorization

$$c = q_1^{g_1} \cdots q_m^{g_m}.$$

Since each $q_i | c$, $q_i | a$ and $q_i | b$, so since irred $\Rightarrow$ prime, $q_i | p_j$ for some j. Since p_j: irred., they are associates, and we must also have $g_i \leq \min(e_j, f_j)$ since q_i can't divide any other p_j's. Cancel, and proceed by induction. $\square$

Thm: R PID $\Rightarrow$ R UFD:

Pf: Let $r \in R$. WTS r has a $\underbrace{\text{unique}}_{b)}$ $\underbrace{\text{prime factorization}}_{a)}$

a) If r irred., done. Otherwise, $r = r_1 s_1$ where r_1, s_1 : nonunits. Treat r_1 and s_1 similarly, and if eventually the process terminates, r has a prime factorization. If the process doesn't terminate, then $\exists$ elts. $r_1, r_2, \dots \in R$ s.t.

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \cdots \subsetneq R.$$

(uses axiom of choice)

Let $I = \bigcup_k (r_k)$; since R is a PID, $I = (a)$ for some $a \in R$. Since $a \in I$, $\exists k$ s.t. $a \in (r_k)$, but then $(r_{k+1}) \subseteq I = (a) \subseteq (r_k)$, a contradiction. Thus, r has a prime factorization.

Corollary of this argument: PIDs are <u>Noetherian</u>
i.e. they don't have an infinite ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$

b) Suppose $r = \underbrace{p_1 \cdots p_n = q_1 \cdots q_m}_{\text{irreds.}}$

Since R is a PID, irred $\Leftrightarrow$ prime. Since $p_1 | r$, $p_1 | q_i$ for some i i.e. $p_1 u = q_i$. Since q_i irred., u is a unit, so p_1, q_i are associates. Cancel to obtain

$$p_2 \cdots p_n = (u^{-1} q_1) \cdots q_{i-1} q_{i+1} \cdots q_m,$$

and proceed by induction. $\square$

Thm (Fermat): Let $p \in \mathbb{Z}$ be an odd prime. Then

$$p = a^2 + b^2,\ a, b \in \mathbb{Z} \iff p \equiv 1 \bmod 4.$$

This expression is unique up to order & sign.

Recall the Euclidean norm $N: \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ given by $N(a+bi) = |a+bi|^2 = a^2 + b^2$

- $N(rs) = N(r)N(s)$ since $|\cdot|$ is multiplicative
- $N(z) = 1 \iff z$ is a unit $\iff z = \pm 1$ or $\pm i$

Lemma: $p = a^2 + b^2 \iff p$ is reducible in $\mathbb{Z}[i]$.

Pf: $\Rightarrow$) If $p = a^2 + b^2$, then in $\mathbb{Z}[i]$,

$p = (a+bi)(a-bi)$, and neither factor is a unit since $N(a \pm bi) = a^2 + b^2 = p \neq 1$.

$\Leftarrow$) Suppose $p = rs$, $r, s \in \mathbb{Z}[i]$ nonunits. Then $p^2 = N(p) = N(r)N(s)$, and since r and s are nonunits $N(r) \neq 1, N(s) \neq 1$, so we must have $N(r) = N(s) = p$. If $r = a+bi$, then $p = N(r) = a^2 + b^2$. $\square$

Pf of Thm.:

$\Rightarrow$ If $p = a^2+b^2$, then $p \equiv a^2+b^2 \bmod 4$. But this is impossible if $p \equiv 3 \bmod 4$ since all squares are $\equiv 0$ or $1 \bmod 4$.

$\Leftarrow$ Let $p \in \mathbb{Z}$ be a prime w/ $p \equiv 1 \bmod 4$, and let $p = 4n+1$. Let $a = (2n)! = (\frac{p-1}{2})!$.

Then

$$
\begin{aligned}
a^2 &= (2n!)^2 (-1)^{2n} \\
&= (2n!)((-2n)(-2n+1)\cdots(-2)(-1)) \\
&\equiv (1 \cdot 2 \cdot \cdots 2n)((2n+1)\cdots(4n)) \\
&= (p-1)! \\
&\equiv -1 \pmod{p}
\end{aligned}
$$

by Wilson's Theorem,

So $p \mid a^2+1$ in $\mathbb{Z}$. If p is irred in $\mathbb{Z}[i]$, p is prime since $\mathbb{Z}[i]$ is a PID. Since

$a^2+1 = (a+i)(a-i)$, we must have $p \mid a+i$ or $p \mid a-i$.
But this is impossible since $p(c+di) = pc + pdi$.
Therefore p is reducible in $\mathbb{Z}[i]$, so by the lemma has the desired form.

Uniqueness is a consequence of unique factorization in $\mathbb{Z}[i]$. $\square$