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

Today: finish Fermat's theorem and prove Gauss' Lemma

Integral domain

HW 1: $\mathbb{Z}[\sqrt{-5}]$ $\quad$ $\mathbb{Z}[\sqrt{-3}]$

$\mathbb{Z}[\sqrt{-5}][x]$ ← lecture 5

UFD (lecture 6): $F[x,y]$ (F: field)

$\mathbb{Z}[x]$ — lecture 3 (not PID) & lecture 5 (UFD)

PID: $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ — D&F p. 277, 282

ED (lecture 2): $\mathbb{Z}$ $\quad$ $\mathbb{Z}[i]$ $\quad$ F $\quad$ $F[x]$

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 $p \equiv a^2+b^2 \mod 4$. But this is impossible if $p \equiv 3 \mod 4$ since all squares are $\equiv 0$ or $1 \mod 4$.

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

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

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 $\mathbb{Z}[i]$. $\square$

Def: R: ring

- The polynomial ring $R[x]$ is the set of polys. in x w/ coeffs. in R:

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}$$

where addition/multiplication are def'n the usual way.

- $p(x) = a_0 + \cdots + a_n x^n \in R[x]$ has <u>degree</u> n. It is <u>monic</u> if $a_n = 1$

- The (multivariate poly. ring $R[x_1, \ldots, x_k]$ is defined inductively: $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$

Remark: $R[x,y] = R[y,x]$

Recall: Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ int. domain

Question: when is $R[x]$ a UFD?

Partial answers:

- If $R = F$: field, then $F[x]$ is a Euclidean domain, w/ norm $N(p(x)) = \deg p$ $\Rightarrow F[x]$: UFD

- If R is not a field, then $R[x]$ is not a PID (but might still be a UFD)

  Pf 1: (r, x) is not principal if r is a nonunit

  Pf 2: (x) is prime, but not maximal since $R[x]/(x) \cong R$ is not a field

- If $R[x]$ is a UFD, then R is a UFD

  Pf: $R \subseteq R[x]$ (constant polys.), and if $p(x)q(x) \in R$, then $p(x), q(x) \in R$

Thm: $R[x]$: UFD $\Leftrightarrow$ R : UFD (next time)

Idea: Factor the polynomial over a field, and show that the factors can be chosen in $R[x]$

e.g.

$$x^2 + x - 2 = \underbrace{(2x-2)\left(\frac{x}{2}+1\right)}_{\in \mathbb{Q}[x]} = \underbrace{(x-1)(x+2)}_{\in \mathbb{Z}[x]}$$

Def: R : int. domain. The <u>field of fractions</u> or <u>quotient field</u> of R is

$$F := \left\{ \frac{a}{b} \,\middle|\, a, b \in R,\ b \neq 0 \right\} \Big/ \ \frac{a}{b} \sim \frac{c}{d} \text{ iff } ad = bc$$

Gauss' Lemma: Let R be a UFD w/ field of fractions F. If $p(x) \in R[x]$ is reducible in $F[x]$, it is reducible in $R[x]$. More precisely, if $p(x) \in R[x]$

$$p = AB, \qquad A, B \in F[x] \quad A, B \text{ nonconstant}$$

then $\exists f \in F$ s.t.

$$a := fA \text{ and } b := f^{-1}B \text{ are in } R[x]$$

(and note that $p = ab$.)

Remark: Converse is false for "silly" reasons:

$2x = 2 \cdot x$ is reducible in $\mathbb{Z}[x]$,

but <u>irreducible</u> in $\mathbb{Q}[x]$ since 2 is a unit.

Pf: Choose $r, s \in R$ s.t. $\tilde{a}(x) := rA(x)$, $\tilde{b}(x) := sB(x) \in R[x]$.

Then

$$d\,p(x) = \tilde{a}(x)\tilde{b}(x) \qquad \text{where } d = rs.$$

If d is a unit (in R), so are r and s, so

$A = r^{-1}\tilde{a}$, $B = s^{-1}\tilde{b} \in R[x]$. Otherwise, take a factorization $d = \underbrace{q_1 \cdots q_n}_{\text{irreds./primes}}$

Let $\overline{R} := R/(q_1)$. Then $\overline{R}[x] = R[x]/\underbrace{(q_1)}_{\substack{\text{prime}\\ \text{ideal}}}$ is an int. domain.

In $\overline{R}[x]$, (WLOG, $\overline{\tilde{a}}(x) = 0$)

$$0 = \overline{d}\,\overline{p}(x) = \overline{\tilde{a}}(x)\overline{\tilde{b}}(x), \text{ so } \overline{\tilde{a}}(x) \text{ or } \overline{\tilde{b}}(x) = 0$$

Then $\tilde{a}(x) = q_1 \hat{a}(x)$ for some $\hat{a} \in R[x]$.

and

$$q_2 \cdots q_n P(x) = \hat{a}(x) \tilde{b}(x)$$

Induction on n proves the result. $\square$