Gauss' Lemma and unique factorization in poly. rings

Integral domain

$\mathbb{Z}[\sqrt{-5}]$ ← HW 1

$\mathbb{Z}[\sqrt{-3}]$

$\mathbb{Z}[\sqrt{-5}][x]$ ← lecture 5,6

UFD

$F[x,y]$

F: field

$\mathbb{Z}[x]$

lecture 3 & lecture 5,6
(not PID) (UFD)

PID

D&F
p.282

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

ED

lecture 2

$\mathbb{Z}$

$\mathbb{Z}[i]$

F

$F[x]$

Recall/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.

- 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

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

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 $\overline{R}[x]$,

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

(WLOG, $\overline{\tilde{a}}(x) = 0$)

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. $\square$

Cor: R : UFD w/ field of fractions F.

Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$.

If $\gcd(a_0, a_1, \ldots, a_n) = 1$, then

$$p \text{ is irred. in } R[x] \iff p \text{ is irred. in } F[x]$$

Pf: $\Rightarrow$) Gauss' Lemma.

$\Leftarrow$) Only possible nontrivial factorization in $R[x]$ that is trivial in $F[x]$ is $p(x) = c\, q(x)$, $c \in R$ nonunit. If $q(x) \in R[x]$, we must have $c \mid a_0, \ldots, c \mid a_n$, but $a_0, \ldots, a_n$ have no nonunit common factors. $\square$

Important special case: If $p(x)$ is monic (top coeff. is 1), then

$$p \text{ is irred. in } R[x] \iff p \text{ is irred. in } F[x]$$