Announcements

Midterm exams are confirmed at

Wednesdays 7:00-8:30pm, Sidney Lu 1043

Integral domain

$\mathbb{Z}[\sqrt{-5}]$ ← HW1 $\quad \mathbb{Z}[\sqrt{-3}]$

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

UFD (lecture 6)

$F[x,y]$ (F: field)

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

PID

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

ED (lecture 2)

$\mathbb{Z}$ $\quad \mathbb{Z}[i]$

F $\quad F[x]$

Last time:

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 $p(x) \in R[x]$ has factorization

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

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

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

(and note that $p = ab$.)

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

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

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 $c | a_0, \ldots, c | a_n$, 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

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

Thm: $R[x]$ is a UFD $\iff$ R is a UFD.

$\Rightarrow$) Last time

$\Leftarrow$) Existance:

Let R be a UFD w/ field of fractions F and let $p(x) \in R[x]$ be nonconstant. Assume that $\gcd(\text{coeffs. of } p) = 1$; otherwise we can factor out this gcd, which has unique factorization in R.

Since $F[x]$ is a UFD (since it is a Euclidean domain), $p(x)$ factors into irreducibles in $F[x]$. By Gauss' Lemma, we can take these factors to be in $R[x]$:

$p(x) = q_1(x) \cdots q_n(x)$ where $q_i(x) \in R[x]$ nonconstant and irred. in $F[x]$.

Since gcd(coeffs of p) $= 1$, for all i we have gcd(coeffs of q_i) $= 1$ since these gcds multiply. Thus, q_i is irred in $R[x]$, and the above is a factorization of $p(x)$ into irreducibles in $R[x]$.

Uniqueness: Let $p = q_1 \cdots q_n = q_1' \cdots q_m'$ be two irred. factorizations for p in $R[x]$. These are also irred. factorizations in $F[x]$ by Gauss' Lemma, so since $F[x]$ is a UFD, we have $m = n$ and, rearranging if necessary, q_i and q_i' are associates i.e. $q_i = \frac{a_i}{b_i} q_i'$ for some $a_i, b_i \in R$.

Clearing denoms., $b_i q_i = a_i q_i' \in R[x]$, and

$\gcd(\text{coeffs. of } b_i q_i) = b_i \cdot \gcd(\text{coeffs. of } q_i) = b_i$

$\gcd(\text{coeffs. of } a_i q_i') = a_i \cdot \gcd(\text{coeffs. of } q_i') = a_i$

Therefore, a_i and b_i are associates, so a_i/b_i is a unit in R, and so q_i and q_i' are associates in $R[x]$, and the factorization is unique. $\square$

Cor: $R[x_1, \ldots, x_n]$ is a UFD $\iff$ R is a UFD

Upshot of all of this: let's mostly consider factorization over a field F.

Goal for rest of today and Wednesday: test when $p \in F[x]$ is irred.

Prop: If $\deg p \leq 3$, then

p is reducible in $F[x]$ $\iff$ p has a root in F

"over F"

Pf: $\Rightarrow$) If p: red. one factor is linear: $ax+b$, so $-b/a$ is a root

$\Leftarrow$) Let $c \in F$ be a root. Since $F[x]$ is Euclidean, we divide p by $x-c$ to get

$$p(x) = q(x)(x-c) + \underbrace{r}_{\in F \text{ since } N(r) < N(x-c) = 1.}$$

Therefore, $p(c) = q(c)(c-c) + r = r$, so $r = 0$, and p is reducible. $\square$

Rational root theorem: Let

$$p(x) = a_n x^n + \dots + a_1 x + a_0 \in \overset{\text{UFD}}{R}[x].$$

Let $r/s \in F[x]$ be a root of p in $\underbrace{\text{lowest terms}}_{\gcd(r,s)=1}$, then $r \mid a_0$ and $s \mid a_n$.

Pf:

$$0 = p(r/s) = a_n (r/s)^n + \dots + a_1 (r/s) + a_0, \text{ so}$$

$$a_n r^n = s(-a_{n-1} r^{n-1} - \dots - a_0 s^{n-1}),$$

so since $\gcd(r,s) = 1$, $s \mid a_n$. Solving for $a_0 s^n$ shows that $r \mid a_0$. $\square$