Announcements

HW2 due Wed. @ 9am

No office hour after class today (was before class)

Integral domain

HW1

$\mathbb{Z}[\sqrt{-5}]$ $\qquad$ $\mathbb{Z}[\sqrt{-3}]$

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

UFD

$F[x,y]$ $\qquad$ $\mathbb{Z}[x]$

F: field

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

PID

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

D&F p.282

ED

lecture 2

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

F $\qquad$ $F[x]$

Unique factorization in poly. rings

Recall:

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 $R[x]$. (If gcd of coeffs. is 1, this is if-and-only-if.) More precisely, if $p \in AB$ in $F[x]$, $\exists f \in F$ s.t. $fA, f^{-1}B \in R[x]$

Thm: $R[x]$ is a UFD $\Leftrightarrow$ 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 $R[x]$:

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

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 $\Longleftrightarrow$ R is a UFD

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

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

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

p is reducible in $F[x]$ $\Longleftrightarrow$ 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

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

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:

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

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

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

Cor: If $p(x) \in R[x]$ is monic, then

$$\begin{array}{c} p \text{ has a root} \\ \text{in } R \end{array} \iff \begin{array}{c} p \text{ has a root} \\ \text{in } F \end{array}$$

E.g: Consider $p(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. We have

$$p(1) = -3 = 0 \qquad\qquad p(-1) = 1 = 0,$$

so by the rational root theorem, p has no roots in $\mathbb{Q}$. Since $\deg p = 3$, it is irred. over $\mathbb{Z}$ or $\mathbb{Q}$.

Prop: R: ring, $I \subsetneq R$ ideal. Let $p(x) \in R[x]$ be a nonconstant <u>monic</u> poly. If $\bar{p}(x)$ is irred in $(R/I)[x]$, then $p(x)$ is irred. in $R[x]$.

Pf: If p is reducible over R, $p = ab$, then $\bar{p} = \bar{a}\bar{b}$, and if p and thus $\bar{p}$ are monic, this is a nontrivial factorization. $\square$

E.g.: $p = x^3 - 3x - 1 \in \mathbb{Z}[x] \rightsquigarrow \bar{p} = x^3 + x + 1$ in $(\mathbb{Z}/2\mathbb{Z})[x]$

$\bar{p}(0) = 1 \neq 0$, $\bar{p}(1) = 1 \neq 0$, so $\bar{p}$ is irred. in $(\mathbb{Z}/2\mathbb{Z})[x]$ hence irred. in $\mathbb{Z}[x]$.

Remark: converse doesn't hold:

$x^4 - 72x^2 + 4$ is reducible in $(\mathbb{Z}/n\mathbb{Z})[x]$ for <u>every</u> n, but irred. in $\mathbb{Z}[x]$.

Eisenstein's Criterion: Let $a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$.
If $p \in \mathbb{Z}$ is a prime s.t.

$$p \mid a_i \ \forall i \text{ and } p^2 \nmid a_0,$$

then a is irred in $\mathbb{Z}[x]$.

Pf (if time):

If $a = b \cdot c$, then $\bar{b} \cdot \bar{c} = \bar{a} = x^n$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.
Let

$$b = x^k + b_{k-1}x^{k-1} + \dots + b_0$$

$$c = x^l + c_{l-1}x^{l-1} + \dots + c_0$$

Then $\overline{b_0} = \overline{c_0} = \overline{0}$ since

$$0 = \overline{a_0} = \overline{b_0}\,\overline{c_0}$$

$$0 = \overline{a_1} = \overline{b_1}\,\overline{c_0} + \overline{b_0}\,\overline{c_1}$$

$$\vdots$$

$$0 = \overline{a_{n-1}} = \overline{b_{k-1}}\,\overline{c_\ell} + \overline{b_k}\,\overline{c_{\ell-1}}$$

$$0 \neq \overline{a_n} = \overline{b_k}\,\overline{c_\ell}$$

But this means that $p \mid b_0$, $p \mid c_0$, so $p^2 \mid a_0$, a contradiction. $\square$

Done with Part I of course: rings and factorization

Next time: on to Chapter 13 and field theory!