Announcements

HW3 posted (due. Wed. 2/12 @ 9am via Gradescope)

HW1 graded (will be released later today)

Let F be a field. Goal for today:

test when $p(x) \in F[x]$ is irred.

Last time:

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

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

Rational root theorem: Let R: UFD, F its field of fractions

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

Let $r/s \in F$ be a root of p in $\underbrace{\text{lowest terms}}_{\gcd(r,s)=1}$,

then $r \mid a_0$ and $s \mid a_n$.

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

p has a root in R $\iff$ p has a root in F

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 $\overline{p}(x)$ is irred in $(R/I)[x]$, then $p(x)$ is irred. in $R[x]$.

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

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

$\overline{p}(0) = 1 \neq 0$, $\overline{p}(1) = 1 \neq 0$, so $\overline{p}$ 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 $\mathbb{Z}[x]$ (and $\mathbb{Q}[x]$)

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

Let
$$b = b_k x^k + b_{k-1}x^{k-1} + \dots + b_0$$
$$c = c_\ell x^\ell + c_{\ell-1}x^{\ell-1} + \dots + c_0$$

Then, applying the polynomial mult. rules:

$$0 = \overline{a_0} = \overline{b_0}\,\overline{c_0} \qquad (0)$$

$$0 = \overline{a_1} = \overline{b_1}\,\overline{c_0} + \overline{b_0}\,\overline{c_1} \qquad (1)$$

$$0 = \overline{a_2} = \overline{b_2}\,\overline{c_0} + \overline{b_1}\,\overline{c_1} + \overline{b_0}\,\overline{c_2} \qquad (2)$$

$$\vdots$$

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

$$0 \neq 1 = \overline{b_k}\,\overline{c_\ell} \qquad (n)$$

top coeff. of $\overline{a}(x)$

Now, since by equation (0) $\overline{b_0}\,\overline{c_0} = 0$, at least one of them is 0. We claim that both are.

WLOG, suppose $\overline{c_0} = 0$, and assume $\overline{b_0} \neq 0$.

By equation (n), $\overline{b_k} \neq 0$, $\overline{c_\ell} \neq 0$, so let i be minimal such that $\overline{c_i} \neq 0$.

Then equation (i) states that

$$\overline{b_0}\,\overline{c_i} + \overline{b_1}\,\overline{c_{i-1}} + \cdots + \overline{b_i}\,\overline{c_0} = 0, \quad (*)$$

where if $i > k$, we set $\overline{b_j} := 0$ for $j > k$.

By assumption, $\overline{c_0} = \cdots = \overline{c_{i-1}} = 0$, so equation (*) becomes

$$\overline{b_0}\,\overline{c_i} = 0,$$

A contradiction, since we have previously assumed that $\overline{b_0}$ and $\overline{c_i}$ are nonzero.

Therefore, we have $\overline{b_0} = \overline{c_0} = 0$, so b_0 and c_0 are multiples of p. Therefore, $a_0 = b_0 c_0$ is a multiple of p^2, contradicting the hypothesis that it's not $\square$

Remark: Essentially the same proof works to prove:

Let $a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$

If $P \subseteq R$ is a prime ideal s.t.

$a_i \in P \ \forall i$ and $a_0 \notin P^2$,

then a is irred in $R[x]$ and $F[x]$ field of fractions

Done with Part I of course: rings and factorization

Small teaser for Chapter 13:

Recall: A field is a comm. ring w/ 1 in which every nonzero elt. has an inverse

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_{p^n}$ (p: prime)

$\mathbb{Q}(x) = \left\{ \begin{matrix} \text{rational} \\ \text{functions} \end{matrix} \ \frac{p(x)}{q(x)}, \ p, q \in \mathbb{Q}[x] \right\} =$ field of fractions of $\mathbb{Q}[x]$

$\mathbb{Q}((t)) = \left\{ \begin{matrix} \text{formal Laurent} \\ \text{power series} \end{matrix} \quad a_n t^n + a_{n+1} t^{n+1} + \dots \quad , n \in \mathbb{Z} \right\}$

$\mathbb{Q}(i)$ "Gaussian rationals"

$\mathbb{Q}(\zeta_n)$ nth root of 1

$\mathbb{Q}(\sqrt{D})$ $D \in \mathbb{Q}$