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 $a(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$

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 $\overline{b} \cdot \overline{c} = \overline{a} = x^n$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

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

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

$$0 = \overline{a_0} = \overline{b_0}\,\overline{c_0}$$
$$0 = \overline{a_1} = \overline{b_1}\,\overline{c_0} + \overline{b_0}\,\overline{c_1}$$
$$0 = \overline{a_2} = \overline{b_2}\,\overline{c_0} + \overline{b_1}\,\overline{c_1} + \overline{b_0}\,\overline{c_2}$$

$$\vdots$$

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

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

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

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

Next time: on to Chapter 13 and field theory!

If extra time:

Field extensions

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)

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

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

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

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

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

Characteristic: Smallest $n>0$ s.t.

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n} = 0 \text{ in } F$$

OR char $F = 0$ if no such n exists

E.g.: char $\mathbb{C}$ = char $\mathbb{Q}$ = char $\mathbb{Q}(\zeta_n) = 0$

char $\mathbb{F}_p$ = char $\mathbb{F}_p(x)$ = char $\mathbb{F}_p((x)) = p$

Prop: $n :=$ char F

a) n is either 0 or prime.

b) If $\alpha \in F$, $n \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{n} = 0$

Pf: a) If $n = ab \neq 0$, then

$$(a \cdot 1) \cdot (b \cdot 1) = (ab \cdot 1) = 0, \text{ so}$$

$a \cdot 1$ or $b \cdot 1$ is 0, contradicting the minimality of n.

b) $\overbrace{\alpha + \cdots + \alpha}^{n} = \alpha(1 + \cdots + 1) = \alpha(0) = 0$ $\square$

Prime subfield: subfield of F generated by 1_F
(smallest subfield of F containg 1)

it is (isom. to) $\begin{cases} \mathbb{Q}, & \text{if } \operatorname{char} F = 0 \\ \mathbb{F}_p, & \text{if } \operatorname{char} F = p \end{cases}$

Def: If K, F are fields w/ $F \subseteq K$, the pair $\underbrace{K/F}_{\text{not a quotient!}}$ is called a <u>field extension</u>

F: base field

K: extension field

Also write $\begin{array}{c} K \\ | \\ F \end{array}$

E.g.: $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathbb{F}_p((t))/\mathbb{F}_p$

$F/$prime subfield of F