Announcements

HW3 posted (due Wed. 2/7)

Midterm 1: Thurs. 2/15 7:00–8:30 pm Loomis Lab. 144

Recall: Irreducibility criteria

R: UFD w/ field of fractions, $p \in R[x]$

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

p is reducible in $\underset{\text{"over } F\text{"}}{F[x]} \iff p$ has a root in F

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 $s \mid a_n$.

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

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

Today: two more criteria, then on to field theory!

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.

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

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

Pf (skip!):

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

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

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

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. $\square$

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)

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

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

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

$F/\text{prime subfield of } F$

Def: A set V is an F-vector space if given $f \in F$, $v \in V$, $f \cdot v \in V$ and

$$f \cdot (v_1 + v_2) = f v_1 + f v_2$$

$$f_1 (f_2 \cdot v) = (f_1 f_2) \cdot v$$

$$(f_1 + f_2) \cdot v = f_1 \cdot v + f_2 \cdot v$$

$$1_F \cdot v = v$$

A basis of V (over F) is a set $S \subseteq V$ s.t.

- Every $v \in V$ can be written

  $$v = f_1 v_1 + \dots + f_n v_n, \quad f_i \in F,\ v_i \in S$$

- If $f_1 v_1 + \dots + f_n v_n = 0$, then $f_1 = \dots = f_n = 0$

  $$f_i \in F,\ v_i \in S$$

The dimension of V over F is $\dim_F V := |S|$

(See D&F §11.1 for more)

Prop: An extension field K of F is a vector space over F

Pf: check axioms

The <u>degree</u> $[K:F] := \dim_F K$

Examples:

a) $\mathbb{C}/\mathbb{R}$: $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$, so

$S = \{1, i\}$, $[\mathbb{C}:\mathbb{R}] = 2$

b) $\mathbb{Q}/\mathbb{Q}(\sqrt{2})$: $\mathbb{Q} = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, so

$S = \{1, \sqrt{2}\}$ $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

c) $\mathbb{F}_p(x)/\mathbb{F}_p$: $1, x, x^2, \dots$ are linearly indep.,

so $[\mathbb{F}_p(x):\mathbb{F}_p] = \infty$