Announcements

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

See Friday's email for full policies

Practice problem sol'n sketches posted

Extra office hour: 10 – 11am tomorrow
   (+20 mins after class today)

HW4: second part will be posted soon (due Wed 2/21)

Midterm 1 review

Partial list of some things we know about:

Classes of integral domain

  fields $\subseteq$ EDs $\subseteq$ PIDs $\subseteq$ UFDs $\subseteq$ Int. doms.
         (plus def'ns and examples)

  Norms (Euclidean, or coming from $\mathbb{C}$)

  Factorizations, gcds, primes, irreducibles, prime/max'l ideals
                    ↑   ⌣   ⌣
               how to   relation   relation
               compute   btwn.   btwn.

    Factorization in $\mathbb{Z}[i]$ $\Leftrightarrow$ writing primes $\in \mathbb{N}$ as $a^2 + b^2$
              (Fermat's Theorem)

Polynomial rings

- Euclidean norm (if over field)
- R UFD $\iff$ $R[x]$ UFD
- Irreducibitiy criteria
    - Gauss' Lemma
    - Test for roots
    - Reduction mod ideal
    - Rational root thm.
    - Eisenstein's criterion
    - Ad-hoc techniques (like plugging in $x+1$

Linear algebra (enough to get by)
- Vector space (over a field), linear independence, span, basis, dimension   (see §11.1)

Field theory
- Characteristic & prime subfield
- Field extension, simple ext'n, degree
- Construction of $F(\alpha)$ ($\cong F(x)/(m_{\alpha,F})$)
- Algebraic vs. transcendental
- Finite vs. infinite

Minimal poly and properties

Tower Law and consequences

Computations in $F(\alpha)$

Other suggestions

Look at lecture notes, hw problems, practice problems

Look at result statements in D&F

Understand all the "little pieces" and be able to fit them together

___

Practice problems (pf. sketches posted on website)

9.3.4) Let $R = \mathbb{Z} + x \mathbb{Q}[x] \subseteq \mathbb{Q}[x]$

$$R = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0 \in \mathbb{Z}, \ a_i \in \mathbb{Q}\}$$

a) Prove that R: int. domain w/ units ± 1

PF: R is a subring (closed under $+, -, \cdot$) so it has no zero-divisors, so is an int. dom.

Let $N : R \to \mathbb{Z}_{\geq 0}$

$\qquad f \mapsto \deg f$ $\qquad\qquad N(fg) = N(f) + N(g)$

All units must have norm 0, so must be a unit in $\mathbb{Z}$, so are ± 1 $\qquad\qquad\qquad$ □

b) Show that the irreds. in R are

$$\{p : \text{prime in } \mathbb{Z}\} \cup \{f(x) \text{ irred. in } \mathbb{Q}[x], \text{ constant term } \pm 1\}$$

Prove that these irreds. are prime in R

Pf: If $p = fg$, $0 = N(p) = N(f) + N(g)$, so $f, g \in \mathbb{Z}$.
Since p is prime in $\mathbb{Z}$, either f or g is a unit.
If $f(x) \in \mathbb{Q}[x]$ is irred in $\mathbb{Q}[x]$ and has constant
term ± 1, if $f = gh$, $g, h \in R$, g and h must have
constant terms ± 1, so if they are nonunits they
have norm $\geqslant 1$. But then f is reducible in $\mathbb{Q}[x]$.

Conversely, if $f(x) \in R$ is irred., then its constant term c
is ± 1 (otherwise $f = p \frac{f(x)}{p}$, for any prime $p \in \mathbb{Z}$
dividing c, is a nontriv. factorization). If f is red
in $\mathbb{Q}[x]$ i.e. $f(x) = g(x) h(x)$, where $g(x)$ has constant
term g_0 and $h(x)$ has constant term $\pm h_0^{-1}$, then
$f(x) = \tilde{g}(x) \tilde{h}(x)$ where $\tilde{g} := \frac{g}{g_0}$, $\tilde{h} : g_0 h \in R$. $\square$

c) Show that x cannot be written as a product of irreds. in R (so R is not a UFD).

Pf: If $x = f_1 f_2 \cdots f_n$ is a product of irreds, then

$$1 = N(x) = N(f_1) + \cdots + N(f_n), \text{ so WLOG,}$$

$N(f_1) = 1, \ N(f_2) = \cdots = N(f_n) = 0.$ We have $f_1 = ax + b,$

but $b = 0$ since otherwise $f_1 \cdots f_n$ would have

nonzero constant term. However, $ax = 2 \cdot \frac{a}{2} x$ is a

nontriv. factorization, so f_1 is not irred. $\qquad \square$

d) Show that x is not prime in R, and describe the quotient ring $R/(x)$.

Pf: In an integral domain, prime $\Rightarrow$ irred.

We claim that

$$R/(x) = \{ \overline{a + bx} \mid a \in \mathbb{Z}, \ b \in \mathbb{Q}, \ 0 \leq b, 1 \} \cong \mathbb{Z} + (\mathbb{Q}/\mathbb{Z}) x$$

No two of these elements differ by a mult of x.

On the other hand, if $f(x) \in R$,

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_0 \in \mathbb{Z}, \ a_i \in \mathbb{Q}$$

$$= a_0 + a_1 x + x \underbrace{\left(a_2 x + \cdots + a_n x^{n-1} \right)}_{\in R}$$

$$= a_0 + \left(a_1 - \lfloor a_1 \rfloor \right) x + x \underbrace{\left(\lfloor a_1 \rfloor + a_2 x + \cdots + a_n x^{n-1} \right)}_{\in R}$$

$$\underset{\text{"floor"}}{\uparrow}$$

$$\mapsto \overline{a_0 + \underbrace{\left(a_1 - \lfloor a_1 \rfloor \right)}_{\in [0, 1)} x}$$

$\square$

13.2.12: Suppose $[K:F]$ is a prime p. If, $F \subseteq E \subseteq K$, then $E = F$ or $E = K$.

Pf: By the Tower Law,

$$p = [K:F] = [K:E][E:F],$$

so either $[K:E] = p$, $[E:F] = 1$, in which case $E = F$, or $[K:E] = 1$, $[E:F] = p$, in which case $E = K$.

$\square$

Side note: In general, if $[K:F] = n$, then the values $[K:E]$ and $[K:F]$ must be factors of n. But unless one of them is 1, we can't say what E is.

We could also ask: If $[k:F]=mn$, does there always exist a field E, $F \subseteq E \subseteq k$ s.t. $[E:F]=m$?

Ans: no, but we need Galois theory!