Announcements

Midterm 2: Thurs. 3/21 7:00–8:30 pm Loomis Lab. 144

Topics: thru. lecture 22 (D&F 14.1)

See email for full policies

Practice problem sol'n sketches posted

Extra office hour after class today

HW7 will be posted soon (due Wed. 3/27)

Midterm 2 review

Integral domains & poly. rings

fields $\subseteq$ EDs $\subseteq$ PIDs $\subseteq$ UFDs $\subseteq$ int. doms.

R UFD $\Leftrightarrow$ $R[x]$ UFD

Irreducibitiy criteria (Gauss' Lemma, Test for roots, Reduction mod ideal, Rational root thm., Eisenstein's criterion, Ad-hoc techniques (e.g. plug in $x+1$))

Field ext'ns

Characteristic & prime subfield

Algebraic vs. transcendental

Finite vs. infinite

Composite ext'ns

Splitting fields & alg. closures (unique up to isom.)

Determine constructibility (degree must be power of 2)

Compute field ext'ns & degrees ← tower law

e.g. cyclotomic ext'ns, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $Sp_{\mathbb{Q}}(x^3-2)$

Compute field autom. & determine if ext'n is Galois

roots of poly must map to each other

Determine whether a poly. is separable

check whether $\gcd(f, Df) = 1$

Computations w/ roots of unity, cyclotomic polys., elts. in field ext'ns, Frobenius map.

Also see Monday's notes p. 1-2 for more on Galois theory

Practice problems (pf. sketches posted on website)

13.4.4) Determine the splitting field and it's degree over $\mathbb{Q}$ for $f(x) = x^6 - 4$.

Sol'n: $K = Sp_{\mathbb{Q}} f$

$$f(x) = (x^3-2)(x^3+2)$$

irred. by Eis.

Roots of x^3-2: $\sqrt[3]{2}$, $\zeta_3 \sqrt[3]{2}$, $\zeta_3^2 \sqrt[3]{2}$

Roots of x^3+2: $-\sqrt[3]{2}$, $-\zeta_3 \sqrt[3]{2}$, $\zeta_3^2 \sqrt[3]{2}$

Thus, $K = Sp\, f = Sp(x^3-2) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$

$[K:\mathbb{Q}] \leq (\deg x^3-2)! = 6$

$$[K:\mathbb{Q}] = \underbrace{[K:\mathbb{Q}(\sqrt[3]{2})]}_{>1}\underbrace{[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]}_{3} = 6$$

13.6.10) Let $\phi = \text{Frob}_p$ on $\mathbb{F}_{p^n}$. Prove that ϕ has order n in $\text{Aut}(\mathbb{F}_p)$.

Pf: Since $\mathbb{F}_{p^n}$ is a finite field, ϕ is an autom.

$|\phi| = n \iff \phi^n = id$ but $\phi^d \neq id$ for $d<n$.

$\phi(a) = a^p$, so $\phi^n(a) = a^{p^n} = a$, since $|\mathbb{F}_{p^n}^\times| = p^n - 1$ and so the order of a in $\mathbb{F}_{p^n}^\times$ must divide p^n-1.

On the other hand, if $\phi^d = id$, then $\phi^d(a) = a\ \forall a \in \mathbb{F}_{p^n}$ i.e. $a^{p^d} - a = 0\ \forall a \in \mathbb{F}_{p^n}$ i.e. every elt. of $\mathbb{F}_{p^n}$ is a root of $x^{p^d}-x$. However, $x^{p^d}-x$ has deg. p^d and $\mathbb{F}_{p^n}$ has p^n elts., so we must have $d \geq n$.

14.1.9) Determine the fixed field of the autom. $\phi : t \mapsto t+1$ of $k(t)$. field

Sol'n: Can check directly that this gives a unique autom:

$$\frac{p(t)}{q(t)} \mapsto \frac{p(t+1)}{q(t+1)}.$$

Let $f(t) = \frac{p}{q} \in k(t)$, where $p, q \in k[t]$, $\gcd(p,q) = 1$, p, q: monic.

If $f(t) = \text{Fix } \phi$, then $f(t+1) = f(t)$, so

$$\frac{p(t+1)}{q(t+1)} = \frac{p(t)}{q(t)} \rightsquigarrow p(t+1)\,q(t) = p(t)\,q(t+1).$$

If $p(t+1) \neq p(t)$, then neither divides the other since they are both monic and have the same degree. But this contradicts $\gcd(p,q) = 1$, so we must have $p(t) = p(t+1)$ and similarly, $q(t) = q(t+1)$.

We have now reduced to finding the set of $f(t) \in k[t]$ s.t. $f(t+1) = f(t)$.

Consider a root $\alpha \in k$ of f (i.e. $f(\alpha) = 0$ in k)
Since $f(t+1) = f(t)$,

$$0 = f(\alpha) = f(\alpha+1) = f(\alpha+2) = \cdots$$

This is impossible in char 0 unless $f(t) \in k$.

In char p, let $\lambda(t) = t(t+1)\cdots(t+p-1) \in k[t]$.

We have $\lambda(t+1) = \lambda(t)$, and any poly. in $k[t]$ gen'd by λ and elts. of k also has this property.

Conversely, let $f(t+1) = f(t)$, $f(0) = a$. Then $g(t) := f(t) - a$ has $g(t+1) = g(t)$, and $g(0) = 0$, so $0 = g(0) = g(1) = \cdots = g(p+1)$, so $\lambda \mid g$. By induction on $\deg f = \deg g$, every f fixed by ϕ is given by an expression in terms of λ and elts. of k.

Conclusion: $\mathrm{Fix}\,\phi = k(\lambda)$ if char $k = p$, $\mathrm{Fix}\,\phi = k$ if char $k = 0$.

adjoin λ to k