Math 100c — Lecture 15 — 5/8/2017

Last Time

* If $F \subseteq L \subseteq K$ is a tower of field extensions,
$$[K:F] = [K:L]\cdot[L:F].$$
* If K/F is an extension & $\alpha \in K$ then
$$\alpha \text{ is alg.}/F \iff [F(\alpha):F] < \infty.$$
* If $\alpha_1, \dots, \alpha_n \in K$ are algebraic $/F$ then $F(\alpha_1, \dots, \alpha_n)/F$ is finite (hence algebraic)

§ 15.6 Adjoining Roots

Let $f(x) \in F[x]$ be an irreducible polynomial / a field F.
Then $\langle f \rangle \subseteq F[x]$ is a maximal ideal, so $F[x]/\langle f \rangle$ is a field. Moreover, we have a map
$$\iota : F \longrightarrow F[x]/\langle f \rangle, \quad a \longmapsto \bar{a}$$
ι is a homom., $\iota(1) = \bar{1}$, & F is a field, so ι is an injection! Moreover, inside $F[x]/\langle f \rangle$ we have $f(\bar{x}) = \overline{f(x)} = 0$, so $\bar{x}$ is a root of f.

Prop Let $f(x) \in F[x]$ be any polynomial. There exists an extension $F \subset K$ st $f(x)$ splits into linear factors in $K[x]$.

Rmk If $F = \mathbb{Q}$ (or $\mathbb{R}$ or $\mathbb{Q}(\sqrt{-3})$ or...) could take $K = \mathbb{C}$.
Less clear if $F = \mathbb{F}_3$ or $F = \mathbb{C}(t)$.

Pf Let $g(x)$ be an irred. factor of $f(x)$ in $F[x]$. Then $g(x)$ (& hence $f(x)$) have a root $\alpha := \bar{x}$ in $F[x]/\langle g \rangle$, which is an extension of f. Over $F[x]/\langle g \rangle$ write $f(x) = (x-\alpha)\cdot f_1(x)$, so that $\deg f_1 = \deg f - 1$. We are done by induction on degree. ∎

Def The <u>derivative</u> of a polynomial $f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x]$ is $f'(x) = n a_n x^{n-1} + \dots + a_1 \in F[x]$.

Prop Let $f(x) \in F[x]$ be a poly. w/ $\deg f > 1$ and let $f'(x)$ be its derivative. TFAE

① f has a multiple root over some extension K of F.

② $\gcd(f, f') \neq 1$.

Pf ① ⇒ ② Let $K \supseteq F$ be an extension such that f splits completely in $K[x]$; write $f(x) = (x-\alpha)^2 \cdot g(x)$ over $K[x]$. Then $f'(x) = 2(x-\alpha)\cdot g(x) + (x-\alpha)^2 \cdot g'(x)$ so $x-\alpha$ is a common divisor of f, f' and $\gcd(f, f') \neq 1$.

② ⇒ ① Let $K \supseteq F$ be an extension st f splits completely in $K[x]$; write $f(x) = c\cdot(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_1, \dots, \alpha_n \in K$ <u>distinct</u>. Then $f' = c(x-\alpha_2)\cdots(x-\alpha_n) + \dots + c(x-\alpha_1)\cdots(x-\alpha_{n-1})$ so that $\gcd(f, f') = 1$ (b/c $(x-\alpha_i) \nmid f'$ for $1 \le i \le n$)

§ 15.7 Finite fields

Let F be a finite field. Then $\operatorname{char} F \neq 0$ so that $\operatorname{char} F = p > 0$ for some prime p and $\mathbb{F}_p \subseteq F$ with $[F : \mathbb{F}_p] = r > 0$.

$\Rightarrow$ All finite fields have prime power order!

Ex $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible (no roots!) so

$$\mathbb{F}_4 := \mathbb{F}_2[x] / \langle x^2+x+1 \rangle$$ is a field of order 4.

elts $(\bar{x} \equiv \alpha)$ $\{0, 1, \alpha, \alpha+1\}$.

$$\alpha^2 \underset{\substack{\uparrow \\ \alpha^2+\alpha+1=0}}{=} -(\alpha+1) \underset{\substack{\uparrow \\ \text{char } 2}}{=} \alpha+1, \text{ etc.}$$

Q How to construct $\mathbb{F}_{2^r}$ (or $\mathbb{F}_{p^r}$) in general?

Trick! Consider $f(x) = x^q - x \in \mathbb{F}_p[x]$ where $q = p^r$.

Then $f'(x) = qx^{q-1} - 1 = -1$ so $\gcd(f, f') = 1$ & f has no multiple roots.

Lem Let $f(x) = x^q - x \in \mathbb{F}_p[x]$ with $q = p^r$ & let $L \supseteq \mathbb{F}_p$ be an ext. st $f(x)$ splits in $L[x]$. Then $K = \{\alpha \in L : f(\alpha) = 0\}$. $|K| = q$ and K is a subfield of L (with $\mathbb{F}_p \subseteq K$).

Cor Let $f(x) \in F[x]$ be an <u>irreducible</u> polynomial.

1. If $f'(x) \neq 0$ then $f(x)$ has no multiple roots in any extension K of F.
2. If $\operatorname{char} F = 0$ then $f(x)$ has no multiple roots in any extension K of F.

Pf (1) We have $\deg f' < \deg f$. Since f is <u>irreducible</u>, if $f' \neq 0$ then $f \nmid f'$ so $\gcd(f, f') = 1$.

(2) If $\operatorname{char} F = 0$ then $f' \neq 0$ whenever $\deg f > 0$. ∎

Rmk Consider the field $F = \mathbb{F}_3(u)$ and let $f(x) = x^3 - u \in F[x]$. Then f is <u>irreducible</u> (u-Eisenstein!) and $f'(x) = p \cdot x^{p-1} - 0 = 0$. Indeed, if $F \subseteq K$ & $\alpha \in K$ is a root of $f(x)$ (so $\alpha^p = u$) then in $K[x]$:

$\cancel{\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}}$ divisible by p

$$\underbrace{\cancel{(x-\alpha)^p}}_{(x-\alpha)^3} = \sum_{i=0}^{\cancel{p}\,3} \binom{\cancel{p}\,3}{i} x^i (-\alpha)^{\cancel{p}\,3-i} \cancel{= \binom{p}{0} x^0 (-\alpha)^p + \binom{p}{p} x^p \alpha^0 = u + x^p}$$

$$= (-\alpha)^3 + x^3 = -u + x^3 = x^3 - u.$$