Lecture 33

(33.0) Recall: for an algebraic extension E/F, E/F is a Galois extension if and only if it is normal and separable. We studied normality in great detail. Now we focus on separability. The following is the main characterization of separable polynomials:

(33.1) Proposition. Let F be a field and $p(x) \in F[x]$. Then $p(x)$ is separable (i.e. has distinct roots in the splitting field of $p(x)$ over F) if, and only if $(p(x), p'(x)) = 1$ in $F[x]$.

Proof. Let E be the splitting extn. of $p(x)$ over F.

$$p(x) = (x-\alpha_1) \cdots (x-\alpha_n) \quad \text{in } E[x]$$

$$(\alpha_1, \ldots, \alpha_n \in E).$$

Then $$p'(x) = \sum_{j=1}^{n} (x-\alpha_1)\cdots(x-\alpha_{j-1}) \overset{\uparrow}{} (x-\alpha_{j+1})\cdots(x-\alpha_n)$$

$x-\alpha_j$ skipped

$$\Rightarrow p'(\alpha_i) = \prod_{\substack{1 \le j \le n \\ j \neq i}} (\alpha_i - \alpha_j)$$

Thus $p(x)$ has repeated roots in $E \iff p'(\alpha_i) = 0$ for some root α_i of $p(x)$.

With this observation in mind, if $(p(x), p'(x)) = 1$ then $\exists\ a(x), b(x) \in F[x]$ s.t.

$$a(x)\,p(x) + b(x)\,p'(x) = 1.$$

If $p(x)$ and $p'(x)$ share a root in E, say $x = \beta$, we will get (setting $x = \beta$) that $0 = 1$, a contradiction. Thus $p(x)$ must have distinct roots.

Conversely, if $d(x)$ is a non constant polynomial dividing both $p(x)$ and $p'(x)$ (in $F[x]$), then $d(x)$ splits completely in $E[x]$ (since $d(x) \mid p(x)$) and every $\beta \in E$ s.t. $d(\beta) = 0$ is a common root of $p(x)$ and $p'(x)$ and hence $p(x)$ has repeated roots in E.

□

(33.2) Characteristic of a field. - Let K be a field

Consider the ring map $\varphi : \mathbb{Z} \longrightarrow K$, $n \longmapsto n.1$

Thus for $n>0$, $\varphi(n) = \underbrace{1+\cdots+1}_{n\text{-times}}$; and $\varphi(-k) = -\varphi(k)$.

Let $p \subset \mathbb{Z}$ be the kernel of φ. As $\mathbb{Z}/p \hookrightarrow K$.

$\mathbb{Z}/p$ must be prime, hence

- either $p = (0)$: in which case we say K has <u>characteristic zero</u>. Moreover, as $\mathbb{Z} \hookrightarrow K$, we get $\mathbb{Q} \longrightarrow K$ (K is an extension of $\mathbb{Q}$).
- or $p = (p)$ for some prime number $p \in \mathbb{Z}_{\geq 2}$. We say K has <u>characteristic</u> p. In this case

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$$

(K is an extension of $\mathbb{F}_p$).

(33.3) Proposition. Let F be an arbitrary field.

(1) If $f(x), g(x) \in F[x]$ are two monic irreducible (distinct) polynomials then f and g have distinct roots in any extension E/F. (i.e. $\nexists\, \alpha \in E$ s.t. $f(\alpha) = g(\alpha) = 0$).

(2) Let $p(x) \in F[x]$ be a monic polynomial.

$$p(x) = f_1(x)^{n_1} \cdots f_r(x)^{n_r} \quad \text{in } F[x]$$

where $f_1, \dots, f_r \in F[x]$ are distinct irreducible monic polynomials, and $n_1, \dots, n_r \in \mathbb{Z}_{\geq 1}$. Then $p(x)$ is separable iff each f_i is separable, and $n_1, \dots, n_r = 1$.

[Remark. - Sometimes people define separability as a condition on irreducible factors which are allowed to have multiplicity.]

Proof. (1) As f, g are distinct, monic and irreducible,

$(f, g) = 1$ (both (f) and (g) are maxl ideals)

$\Rightarrow \exists\ a(x), b(x) \in F[x]$ s.t. $a(x) f(x) + b(x) g(x) = 1$.

But if in some E/F, $\beta \in E$ is a common root of f & g, we would get $0 = 1$ by setting $x = \beta$.

(2) follows immediately from (1). □

(33.4) Definition A field K is called <u>perfect</u> if every irreducible $f(x) \in K[x]$ is separable (i.e. $(f, f') = 1$)

K is said to be <u>imperfect</u> otherwise

Lemma. K is imperfect $\Rightarrow$ $\mathrm{Char}(K) \neq 0$.

[Sorry: read - every field of characteristic 0 is perfect.]

Proof. Let $g(X) \in K[X]$ be irreducible polynomial. (& monic)

Then, as degree$(g'(X)) < \deg(g(X))$, the gcd of $g(x)$ and $g'(X)$ is not 1 $\Leftrightarrow$ $g'(X) = 0$.

$$g(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K \not\in [X]$$

$$g'(X) = nX^{n-1} + a_{n-1}(n-1)X^{n-2} + \dots + a_1 = 0$$

Coeff. of X^k in $g'(X)$ $= a_{k+1}(k+1) = 0$

means either $a_{k+1} = 0$ in $\not\in K$ (i.e. coeff. of X^{k+1} in $g(X)$ is 0)

or $(k+1)\cdot 1 = 0$ in $\not\in K$ (i.e. $p \mid (k+1)$ where $p \neq 0$ (has to be) char(K))

Thus not only Char$(K) = p \neq 0$, but also

$$g(X) \in K[X^p].$$

□

(33.5) Let us fix a prime $p \in \mathbb{Z}_{\geq 2}$.

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$ is a finite field of char. p.

Any field of characteristic p is an extn. (algebraic or not)

of $\mathbb{F}_p$. Let $K/\mathbb{F}_p$ be a field of characteristic p.

Proposition. (1) $\sigma_p : K \longrightarrow K$, $x \longmapsto x^p$

is a morphism of fields over $\mathbb{F}_p$.

(2) $K/\mathbb{F}_p$ finite $\Rightarrow |K| = q = p^r$ where $r = (K : \mathbb{F}_p)$.

In this case K = splitting extn. of $X^q - X \in \mathbb{F}_p[X]$.

(3) Every finite field is perfect.

Proof (1) $\sigma_p(0) = 0$ and $\sigma_p(1) = 1$. Also $\sigma_p(ab) = \sigma_p(a)\sigma_p(b)$.

The only non-trivial identity is

$$\sigma_p(a+b) = (a+b)^p = a^p + p \cdot a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \dots + b^p$$

$$= a^p + b^p \quad \text{because } p \text{ divides } \binom{p}{k} \quad (1 \le k \le p-1)$$

$$= \sigma_p(a) + \sigma_p(b)$$

It remains to show that $a^p = a \ \forall\ a \in \mathbb{F}_p$. This is true, and needed for later, to show for any finite field.

Claim: Let F be a finite field and $q = |F|$.
$(|F| < \infty)$

Then $a^{q-1} = 1 \quad \forall\ a \in F \setminus \{0\}$.

Proof $F^\times = F \setminus \{0\}$ is an abelian group of size $q-1$.

So $\text{ord}(a) \mid (q-1) \quad \forall\ a \in F^\times$.

(2). Clearly if $(K : \mathbb{F}_p) = r$, $|K| = p^r (= q)$.

Now there are q solutions (distinct) of $X^q - X = 0$, in K.
(by Claim)

$$\Rightarrow X^q - X = X(X-1) \cdot \prod_{a \in K \setminus \{0,1\}} (X-a)$$

$\Rightarrow K$ is the splitting extn. of $X^q - X = 0$ over $\mathbb{F}_p$.

(In particular there is only one field of size p^r)
(uniqueness of splitting extn.) ↳ and $K/\mathbb{F}_p$ is Galois!

(3) Let K be the (see (2) above) field of size $q = p^r$.

If $g(X) \in K[X]$ is an irreducible polynomial, and

L = splitting extn. of g over K, then $|L| < \infty$ and

hence $|L| = \tilde{q} = p^{rn}$. As $\mathbb{F}_p \subset K \subset L$ and $L/\mathbb{F}_p$ is Galois

We get that L/K is Galois $\Rightarrow$ $g(X)$ is separable. $\square$

(33.6) In conclusion, to find an irreducible, non-separable polynomial, one must first take coefficients from an infinite field of characteristic $p \neq 0$. e.g. $K = \mathbb{F}_p(\lambda)$.

Moreover such a polynomial has to be a polynomial in X^p.

This leads to the easiest example of irred. non-separable:

$$f(X) = X^p - \lambda \in K[X]$$

If L is its splitting extn. (of Char p again) and $\mu \in L$ is such that $\mu^p = \lambda$, then

$$(X^p - \lambda) = (X - \mu)^p \text{ in } L$$

i.e. $$L \simeq K(\lambda^{\frac{1}{p}}) = K[T]/(T^p - \lambda).$$