403/503 - L39

[§ 22.1 in Judson]

Finite fields.

Def If the order of 1_R in the additive group $(R,+)$ of a ring is $n < \infty$, we say R has *characteristic n* and write $\operatorname{char} R = n$.

If 1_R has infinite order in $(R,+)$ we say R has *characteristic zero* and write $\operatorname{char} R = 0$.

Lem If R is an integral domain then either $\operatorname{char} R = 0$ or $\operatorname{char} R = p$, p prime.

Prop If F is a finite field, of characteristic p, then $|F| = p^n$, some $n > 0$.

Pf $\phi : \mathbb{Z} \to F$ $\quad \ker \phi = p\mathbb{Z}$

$[F : \mathbb{Z}_p] = n$

Freshman's Dream (e.g. integral domain)

Let p prime and D a comm ring of characteristic p. Then

$$(a+b)^p = a^p + b^p$$

(and thus more generally: $(a+b)^{p^n} = a^{p^n} + b^{p^n} \ \forall n \geq 0$)

Pf $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, $p \nmid k!(p-k)!$ when $0 < k \leq p-1$

so $p \mid \binom{p}{k}$.

Cor If D is a comm ring of char p then $\phi_p : D \to D$, $\phi(a) = a^p$, is an endomorphism

Def ϕ_p is the Frobenius Endomorphism

Note: Always injective when D is a field.

~~505 / 514~~

13.5 Separability

Def $f(x) \in F[x]$ is *separable* if when factored over a splitting field

$$f(x) = (x-\alpha_1)^{n_1} \cdots (x_k-\alpha_k)^{n_k}$$

we have $n_1 = \cdots = n_k = 1$. otherwise $f(x)$ is *insepara*

Note: Doesn't depend on splitting field.

Ex $x^{2+t} = x^{2-t}$ over $F = \mathbb{F}_2(t)$ is irreducible but inseparable: If $\sqrt{t}$ denotes a root in an extension then $(x^2+t) = (x+\sqrt{t})^2$

Prp 33 $f(x)$ has a multiple root α iff α is also a root of $D_x f(x)$.

↘ formal derivative.

Thus $f(x)$ is separable iff $(f(x), D_x f(x)) = 1$

proof $f'(x) = D_x((x-\alpha)^n \cdot \tilde{f}(x)) = n(x-\alpha)^{n-1}\tilde{f}(x) + (x-\alpha)^n$

if $n > 1$ then α is a root of this

conversely if $n = 1$ then

$f'(\alpha) = \tilde{f}(\alpha) + 0 \neq 0$

QE

Ex 1) $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$

$D_x f(x) = p^n x^{p^n - 1} - 1 = -1$ no roots

$\Rightarrow$ $f(x)$ separable.

2) $f(x) = x^n - 1$ over $\mathbb{Q}$ (or any F, $\operatorname{char} F = p \nmid n$)

$D_x f(x) = n x^{n-1}$ only 0 is a root, and $f(0) \neq 0$

hence $f(x)$ is separable.

3) If $\operatorname{char} F = p$ and $p \mid n$ then $f(x) = x^n -$ is inseparable since $D_x f(x) = 0$

Cor 34 Every irr. pol over a field of char 0 is separable.

In fact a pol $f(x) \in F[x]$, $\operatorname{char} F = 0$, is separable iff $f(x)$ is a product of distinct irr. factors $f_i(x) \in F[x]$.

Proof: If $\deg f(x) = n$, then $\deg D_x f(x) =$ since $\operatorname{char} F = 0$. Since $f(x)$ is the only factor are 1 and $f(x)$. These imply $(f(x), D_x f(x)) = 1$.

Last claim follows from that distinct irr pols have no roots in common (in an alg closure say). QED.

Prp 35 Char $F = p$ Then

$$\varphi_p : F \to F, \quad \varphi(\alpha) = \alpha^p$$

is a monomorphism called the Frobenius endomorphism.

pf. $p \mid \frac{p!}{k!(p-k)!}$ if $1 \le k \le p-1$

So binomial formula implies $\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta)$.
$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ and $\varphi(1) = 1$ are obvious.
F field $\Rightarrow \varphi$ injective. QED.

Cor 36. If $\mathbb{F}$ is a finite field of char $\mathbb{F} = p$, then φ_p is an automorphism, hence any element of $\mathbb{F}$ has the form α^p, for some $\alpha \in \mathbb{F}$.

pf φ_p injective, $\dim_{\mathbb{F}_p} \mathbb{F} < \infty \Rightarrow \varphi_p$ automorphism QED

Def A field K is perfect if $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ and $\varphi_p : K \to K$ is surjective ($\Leftrightarrow$ automorphism)

Thm Let F be a perfect field and $f(x) \in F[x]$ an irreducible polynomial over F. Then $f(x)$ is separable.

(**Proof**) If $\operatorname{char} F = 0$, follows by Cor 34.

Suppose $\operatorname{char} F = p$ and that $\varphi_p : F \to F$, surjective. Suppose $f(x) \in F[x]$ is inseparable. WTS $f(x)$ is reducible.

By Prp 33, $(f(x), D_x f(x)) \neq 1$, so if $f(x)$ we irreducible, $(f(x), D_x f(x)) = f(x)$.

But $\deg D_x f(x) < \deg f(x)$. Hence $D_x f(x$

Write $f(x) = \sum_{k=0}^{n} a_k x^k$, $D_x f(x) = \sum_{k=1}^{n} k a_k x$

So $a_k \neq 0 \Rightarrow p \mid k$, hence $f(x) = g(x^p)$ f some $g(x) \in F[x]$.

Write $g(x) = \sum_{i=0}^{m} b_i x^{pi}$.

Since F is perfect, $b_i = \varphi_p(b_i') = (b_i')^p$ for some $b_i' \in F$. Thus

$$f(x) = g(x^p) = \sum_{i=0}^{m} (b_i' x^i)^p = \left(\sum_{i=0}^{m} b_i' x^i\right)^p$$

Sinc char $F = p$. This contradicts that $f(x)$ is irreducible.

Q.E.D.