Before proving it, let's look at ...

EXAMPLES:

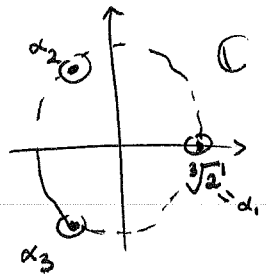
① $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ does not split completely in $\mathbb{Q}(\sqrt[3]{2})[x]$

$= (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$

but it does split completely in $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$

$\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$

$\omega = e^{2\pi i/3}$



as $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$.

We could have guessed $\alpha_1, \alpha_2, \alpha_3$ were distinct ahead of time because $\gcd(f(x), f'(x)) = \gcd(x^3-2, 3x^2) = 1$

3/27/2019

② On the other hand, $f(x) = x^3 - 3x^2 + 4 \in \mathbb{Q}[x]$

has $f'(x) = 3x^2 - 6x = 3x(x-2)$

which has $x-2$ dividing $\gcd(f(x), f'(x))$ since $f(2) = 8 - 3\cdot 4 + 4 = 0$

(in fact $x-2 = \gcd(f(x), f'(x))$).

Hence $f(x)$ must have repeated roots, and can check $f(x) = (x-2)^2(x+1)$

③ $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ does not split completely in $\mathbb{F}_2[x]$

but it does in $\mathbb{F}_4[x]$ where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$

$= \{0, 1, \alpha, \alpha+1\}$

as $f(x) = (x+\alpha)(x+\alpha+1)$ $(= (x-\alpha)(x-(\alpha+1)))$

It had distinct roots since $f'(x) = 2x+1 = 1$ has $\gcd(f(x), f'(x)) = 1$

But $g(x) = x^4 + x^2 + 1 = (x^2+x+1)^2$ in $\mathbb{F}_2[x]$

does not have distinct roots in $\mathbb{F}_4[x]$: $g(x) = (x-\alpha)^2(x-(\alpha+1))^2$,

which was predictable from $f'(x) = 4x^3 + 2x = 0$

so $\gcd(f(x), f'(x)) = f(x) = x^4 + x^2 + 1 \neq 1$.

(Note $g(x) = f(x^2)$ where $f(x) = x^2 + x + 1$ from above)

(4) $\mathbb{F} = \mathbb{F}_p(u)$ = rational functions in u over $\mathbb{F}_p$

has $f(x) = x^p - u \in \mathbb{F}[x] = \mathbb{F}_p(u)[x]$ irreducible (not obvious, but can be deduced from Eisenstein at the prime ideal (u) inside $\mathbb{F}_p[u]$)

so it doesn't split into linear factors in $\mathbb{F}_p(u)[x]$,

but $f'(x) = px^{p-1} = 0$ so $\gcd(f(x), f'(x)) = f(x) = x^p - u \neq 1$

and hence it must have ~~exactly~~ repeated roots in any extension where it splits (see EXER. 16.3.3 for the $p=2$ case).

proof of PROP:

(a): Given $f(x) \in \mathbb{F}[x]$, prove $\exists\ \mathbb{K} \supset \mathbb{F}$ where it splits completely by induction on $\deg(f)$: either $\mathbb{F}$ itself works, or $f(x)$ has an irreducible factor $g(x)$ that doesn't split in $\mathbb{F}[x]$,

so $\mathbb{F}' := \mathbb{F}[x]/(g(x))$ is an extension of $\mathbb{F}$ containing $\alpha := \overline{x}$ as a root of $g(x)$

Thus $f(x) = g(x)h(x)$ in $\mathbb{F}[x]$ for some $h(x) \in \mathbb{F}[x]$

$= (x-\alpha)\,\tilde{g}(x)h(x)$ in $\mathbb{F}'[x]$ for some $\tilde{g}(x) \in \mathbb{F}'[x]$

and now apply induction to $\tilde{g}(x)h(x)$, which has lower-degree.

(b): First note that $\gcd_{\mathbb{K}[x]}(f(x), f'(x)) = \gcd_{\mathbb{F}[x]}(f(x), f'(x))$

since one can compute gcd's via Euclid's algorithm: $f(x) = f'(x)\,g(x) + r(x)$

$$\gcd(f(x), f'(x)) = \gcd(r(x), f'(x)) = \dots$$

(same answers in $\mathbb{F}[x]$ or $\mathbb{K}[x]$ by uniqueness of polynomial division)

Then once $f(x)$ splits completely in $\mathbb{K}$, for a given root α of $f(x)$, it will have multiplicity m exactly if $f(x) = (x-\alpha)^m g(x)$ with $g(\alpha) \neq 0$

so $f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$

$= (x-\alpha)^{m-1}\underbrace{[m\,g(x) + (x-\alpha)g'(x)]}_{h(x) \text{ having } h(\alpha) = m\,g(\alpha)}$

Thus $m \geq 2 \Rightarrow x-\alpha$ divides $\gcd(f(x), f'(x))$

$m = 1 \Rightarrow f'(x) = h(x)$ with $h(\alpha) = g(\alpha) \neq 0$, so no root of $f(x)$ divides $f'(x)$, i.e. $\gcd(f, f') = 1$.

(c): When $f(x)$ is irreducible in $\mathbb{F}[x]$, since $\deg(f'(x)) < \deg(f(x)) =: n$, one has $\gcd(f(x), f'(x)) = 1$, unless $f'(x) = 0$

But $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \neq 0$

has $f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 = \sum_{i=1}^{n} i a_i x^{i-1} = 0$

$\iff$ $\mathrm{char}(\mathbb{F}) = p$ and p divides $i a_i$ $\forall i = 1, \ldots, n$

i.e. $a_i \neq 0 \Rightarrow p$ divides i

so $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + a_{3p} x^{3p} + \cdots + a_{mp} x^{mp}$

$= a_0 + a_p x^p + a_{2p} (x^p)^2 + a_{3p} (x^p)^3 + \cdots + a_{mp} (x^p)^m$

$= g(x^p)$ where $g(x) = a_0 + a_p x + a_{2p} x^2 + \cdots + a_{mp} x^m$ ∎

§15.7 Finite fields

We've already seen that a finite field $\mathbb{F}$

- has $\mathrm{char}(\mathbb{F}) = p$ a prime, so $\mathbb{F}_p \subset \mathbb{F}$
- if $[\mathbb{F} : \mathbb{F}_p] = d$ then $|\mathbb{F}| = p^d =: q$, a prime power
- $\mathbb{F}^\times = \mathbb{F} - \{0\} = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-2}\} \cong \mathbb{Z}/(q-1)\mathbb{Z}$ cyclic ($\gamma^{q-1} = 1$)

but we haven't yet seen

- that such an $\mathbb{F}$ exists for every size $q = p^d$ with $d \in \{1, 2, \ldots\}$
- they're all isomorphic when they have the same size q (so we could call them all "$\mathbb{F}_q$")

Let's combine these with some other amazing properties into one big theorem.

THEOREM: (15.7.3, 15.7.4) Fix a prime power $q = p^d$ with $d \in \{1, 2, \ldots\}$.

(a) $\exists$ an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d, and hence a finite field $\mathbb{F} := \mathbb{F}_p[x]/(f(x))$ with $|\mathbb{F}| = q = p^d$

(b) They are all isomorphic (as rings/fields), so we can call any of them $\mathbb{F}_q$.

(c) Any such $\mathbb{F}_q$ has the Frobenius map $\mathbb{F}_q \xrightarrow{F} \mathbb{F}_q$, $\alpha \longmapsto \alpha^p$

giving an $\mathbb{F}_p$-automorphism of $\mathbb{F}_q$

(d) $\mathbb{F}_q$ is the set of all the (distinct!) roots of $x^q - x$ inside any extension $\mathbb{K} \supset \mathbb{F}_p$ where it splits, i.e. $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

Equivalently, $\mathbb{F}_q = \{\alpha \in \mathbb{K} : \underbrace{\alpha^q}_{(((\alpha^p)^p)\cdots)^p} = \alpha\} = \{\alpha \in \mathbb{K} : \underbrace{(F \circ F \circ \cdots \circ F)}_{F^d}(\alpha) = \alpha\}$

(e) Inside $\mathbb{F}_p[x]$, the irreducible factorization of $x^q - x$ is

$$x^q - x = \prod_{\substack{\text{all irreducibles} \\ g(x) \in \mathbb{F}_p[x] \\ \text{with } \deg(g) \text{ dividing } d}} g(x)$$

(f) $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d} \iff e$ divides d

3/29/2019

EXAMPLES: Let's examine $\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}$, by first cataloguing irreducibles in $\mathbb{F}_2[x]$ up to degree 4:

$\cap$ $\quad$ $=$ $\quad$ $=$

$\mathbb{F}_8 = \mathbb{F}_{2^3}$ $\quad$ $\mathbb{F}_4$ $\quad$ $\mathbb{F}_{16}$

degree:	1	2	3	4
	x	~~$x^2+1 = (x+1)^2$~~	~~$x^3+1 = (x+1)(x^2+x+1)$~~	x^4+x+1
	$x+1$	x^2+x+1	x^3+x+1	~~$x^4+x^2+1 = (x^2+x+1)^2$~~
			x^3+x^2+1	x^4+x^3+1
			~~$x^3+x^2+x+1 = (x+1)^3$~~	$x^4+x^3+x^2+x+1$