Math 5402

5/6/20

- One 8.5 x 11 sheet (one-sided) notes. Just thm statements / defs. No proofs or calculations.

Galois group of finite fields

$\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p = \mathbb{Z}_p$. So, $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$. Therefore,

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = |\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$$
$$= [\mathbb{F}_{p^n} : \mathbb{F}_p].$$

$\boxed{\text{Claim:}}$ $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$

Since $\mathbb{F}_{p^n}$ and $\mathbb{F}_p$ are finite, there is a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. [Worst case the basis is all of $\mathbb{F}_{p^n}$.]

Suppose $\beta_1, \beta_2, \ldots, \beta_k$ is a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. That is,

$$\mathbb{F}_{p^n} = \{ a_1\beta_1 + a_2\beta_2 + \cdots + a_k\beta_k \mid a_i \in \mathbb{F}_p \}$$

(each a_i has p choices)

this set has p^k elements

So,

$$p^n = |\mathbb{F}_{p^n}| = p^k$$

Thus, $k = n$. $\boxed{\text{Claim}}$

Thus, $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$

Consider the Frobenius automorphism

$\sigma_p : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ where $\sigma_p(x) = x^p$.

We proved that σ_p is an isomorphism. (13.5)

Also, if $f \in \mathbb{F}_p$, then $f^p = f$.

Why? $\bar{0}^p = \bar{0}$. If $f \neq \bar{0}$, then $f \in \mathbb{F}_p^\times$ and $\mathbb{F}_p^\times = \mathbb{Z}_p^\times$ is a group under mult, of size $p-1$. So, $f^{p-1} = \bar{1}$. So, $f^p = f$.

So, $\sigma_p(f) = f^p = f$ for all $f \in \mathbb{F}_p$.

Thus, $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$.

Note that

$$\sigma_p^k(x) = \left(\left((x^p)^p\right)\cdots\right)^p = x^{p^k}$$

We know $x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}$ is precisely the roots of $x^{p^n} - x = 0$ (13.5)

So, the order of σ_p in $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$ is at most n. [Since $\sigma_p^n =$ identity]

We cannot have $\sigma_p^k = \text{identity}$ for $1 \le k < n$ since then

$x^{p^k} - x = 0$ for all $x \in \mathbb{F}_{p^n}$.

But $x^{p^k} - x$ has no multiple roots [its derivative is -1]. So it has at most p^k roots in $\mathbb{F}_{p^n}$. Not enough roots to make all of $\mathbb{F}_{p^n}$.

Therefore, σ_p has order n and

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$$
$$= \{1, \sigma_p, \sigma_p^2, \ldots, \sigma_p^{n-1}\}.$$

$\boxed{\text{END}}$

HW 14.1 #C

$x^2 + x + \bar{1}$ is irreducible over $\mathbb{Z}_2$.

So, $\mathbb{F}_4 = \mathbb{Z}_2[x] / (x^2 + x + \bar{1}) = \mathbb{Z}_2[x]/I$

$= \{ \bar{0} + I,\ \bar{1} + I,\ x + I,\ (\bar{1} + x) + I \}$

$I = (x^2 + x + \bar{1})$

$(x^2 + x + \bar{1}) + I = \bar{0} + I \rightarrow x^2 + I = (-\bar{1} - x) + I$

$= (\bar{1} + x) + I$ $\mathbb{Z}_2$

$\mathrm{Gal}(\mathbb{F}_4 / \mathbb{F}_2) = \langle \sigma_2 \rangle = \{ i, \sigma_2 \}$

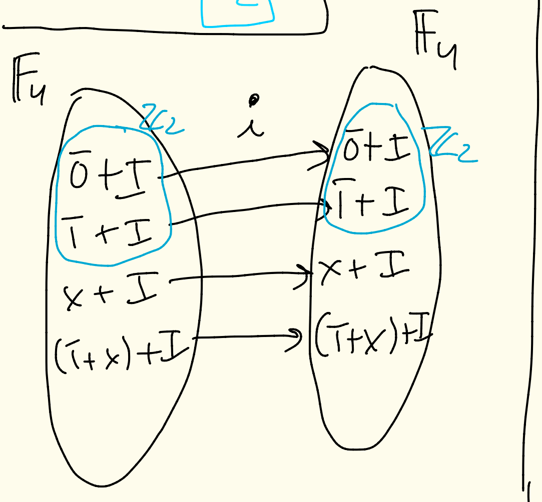
$4 = 2^{2}$ ← order of σ_2 ; 2 ← σ_2

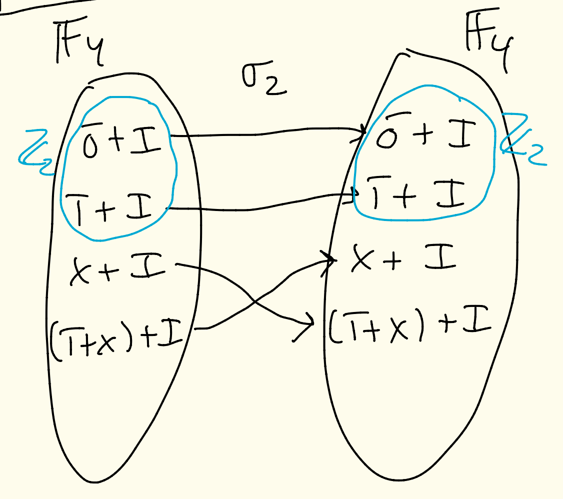
$\boxed{\sigma_2(x) = x^2}$

$(x + I)^2 = x^2 + I = (x + \bar{1}) + I$

$(\bar{1} + x)^2 + I = \bar{1} + \bar{2}x + x^2 + I$

$= \bar{1} + \bar{0} + \bar{1} + x + I = x + I$





$\boxed{14.2}$

pg 6

Thm: The extension K/F is Galois iff K is the splitting field of some seperable polynomial over F.

Galois means: $|Aut(K/F)| = [K:F]$

separable: no repeated/multiple roots

Ex: Find Galois group for

x^6-1 over $\mathbb{Q}$.

roots: $1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5$ where

$$\zeta_6 = e^{2\pi i/6} = e^{\pi i/3} = \cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)$$
$$= \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$K = \mathbb{Q}(\zeta_6)$ is the splitting field of the separable polynomial x^6-1 over $\mathbb{Q}$.

So, $\mathrm{Gal}(K/\mathbb{Q})$ is Galois and

$$|\mathrm{Gal}(K/\mathbb{Q})| = [K:\mathbb{Q}] = [\mathbb{Q}(\zeta_6):\mathbb{Q}]$$
$$= \deg(m_{\zeta_6,\mathbb{Q}}(x)) = \deg(\Phi_6(x))$$
$$= 2$$

$$x^6-1 = \Phi_1\Phi_2\Phi_3\Phi_6$$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)}$$
$$= x^2-x+1$$

If $\sigma \in Gal(\mathbb{Q}(\zeta_6)/\mathbb{Q})$ we just need to calculate $\sigma(\zeta_6)$ which must be a root of $\min_{\zeta_6,\mathbb{Q}}(x) = \Phi_6(x)$

$$= \prod_{\substack{1 \le a \le 6 \\ \gcd(a,6)=1}} (x - \zeta_6^a)$$

$$= (x - \zeta_6^1)(x - \zeta_6^5)$$

Another way to get $\deg(\Phi_6) = 2$

So, $\sigma(\zeta_6) = \zeta_6$ or $\sigma(\zeta_6) = \zeta_6^5$.

$$\mathbb{Q}(\zeta_6) = \{a + b\zeta_6 \mid a, b \in \mathbb{Q}\}$$

$$Gal(\mathbb{Q}(\zeta_6)/\mathbb{Q}) = \{i, \sigma\}$$

where $i(a + b\zeta_6) = a + b\zeta_6$

$\sigma(a + b\zeta_6) = a + b\zeta_6^5$

extra simplification

$$\zeta_6^2 - \zeta_6 + 1 = 0$$
$$\zeta_6^2 = \zeta_6 - 1$$

$$= a + b\zeta_6^2\zeta_6^2\zeta_6$$
$$= a + b(\zeta_6 - 1)(\zeta_6 - 1)\zeta_6 = \dots$$