20250426 MATH4302 Assignment 6

(7) (a) Definition: Let $K \subseteq L$ be a field extension. Define $\mathrm{Aut}_K(L)$ as the set of all L-automorphism σ with $\forall k \in K, \sigma(k) = k$.

(Group Structure) Proposition: $\mathrm{Aut}_K(L)$ is a subgroup of $\mathrm{Aut}(L)$.

Proof: $\forall k \in K, \mathrm{id}_L(k) = k$, so $\mathrm{id}_L \in \mathrm{Aut}_K(L)$

$\sigma, \tau \in \mathrm{Aut}_K(L) \Rightarrow \forall k \in K, \sigma(k) = \tau(k) = k$

$\Rightarrow \forall k \in K, \sigma\tau(k) = k \Rightarrow \sigma\tau \in \mathrm{Aut}_K(L)$

$\sigma \in \mathrm{Aut}_K(L) \Rightarrow \forall k \in K, \sigma(k) = k \Rightarrow \forall k \in K, \sigma^{-1}(k) = k \Rightarrow \sigma^{-1} \in \mathrm{Aut}_K(L)$

(Group Action Structure) Proposition: If $k(x) \in K[x]$, and $Z_L(k(x)) = \{l \in L : k(l) = 0\}$, then $\mathrm{Aut}_K(L)$ acts on $Z_L(k(x))$ by evaluation.

Proof: Assume that $k(x) = k_0 + k_1 x + \cdots + k_n x^n$.
($k_0, k_1, \ldots, k_n \in K$)

$\sigma \in \mathrm{Aut}_K(L)$ and $l \in Z_L(k(x))$

$\Rightarrow k_0 + k_1 l + \cdots + k_n l^n = 0$

$\Rightarrow k_0 + k_1 \sigma(l) + \cdots + k_n \sigma(l)^n = \sigma(k_0 + k_1 l + \cdots + k_n l^n) = \sigma(0) = 0$

$\Rightarrow \sigma(l) \in Z_L(k(x))$, so the action map is well-defined

$l \in Z_L(k(x)) \Rightarrow \mathrm{id}_L(l) = l$

$\sigma, \tau \in \mathrm{Aut}_K(L)$ and $l \in Z_L(k(x)) \Rightarrow \sigma\tau(l) = \sigma(\tau(l))$

(Embedding into S_n) Proposition: If $k(x) \in K[x]$, and $L = K[Z_L(k(x))]$, then $\mathrm{Aut}_K(L)$ is embedded in $\mathrm{Perm}(Z_L(k(x)))$.

In particular, if $K \subseteq L$ is a finite extension, then take a basis $l_1, l_2, \ldots, l_m$ of L over K, take minimal polynomials $k_1(x), k_2(x), \ldots, k_m(x)$ of $l_1, l_2, \ldots, l_m$ over K, and $\mathrm{Aut}_K(L)$ is embedded in $\mathrm{Perm}(Z_L(k(x)k_2(x)\cdots k_m(x))) = S_n$, which implies $\mathrm{Aut}_K(L)$ is a finite group.

Date

Proof: It suffices to show that:

$$\forall l \in Z_L(k(x)),\ \sigma(l) = l$$

$$\Rightarrow \forall l \in K[Z_L(k(x))] = L$$

$$\sigma(l) = \sigma\Big(\sum_{\mu_1,\mu_2,\cdots,\mu_n} a_{\mu_1,\mu_2,\cdots,\mu_n} l_1^{\mu_1} l_2^{\mu_2} \cdots l_n^{\mu_n}\Big)$$

$$= \sum_{\mu_1,\mu_2,\cdots,\mu_n} a_{\mu_1,\mu_2,\cdots,\mu_n} \sigma(l_1)^{\mu_1} \sigma(l_2)^{\mu_2} \cdots \sigma(l_n)^{\mu_n}$$

$$= \sum_{\mu_1,\mu_2,\cdots,\mu_n} a_{\mu_1,\mu_2,\cdots,\mu_n} l_1^{\mu_1} l_2^{\mu_2} \cdots l_n^{\mu_n} = l$$

$$\Rightarrow l = id_L$$

(b) Proposition: Let $k(x) \in K[x]$ be an irreducible polynomial, and $L = K[x]/\langle k(x)\rangle$. The group $Aut_K(L)$ acts transitively on $Z_L(k(t))$.

In particular, $|Aut_K(L)| = |Z_L(k(t))| \le \deg k(t) = [L:K]$

(Simple Extension ↓ Transitive Action)

Proof: For all $l_1, l_2 \in Z_L(k(t))$, there are field isomorphisms:

$$\sigma_1: K[x]/\langle k(x)\rangle \to K[l_1],\ f(\bar{x}) = f(l_1)$$

$$\sigma_2: K[x]/\langle k(x)\rangle \to K[l_2],\ f(\bar{x}) = f(l_2)$$

because $l_1, l_2 \in L$ share the same irreducible polynomial $k(t)$ over K.

This implies $\underbrace{\sigma_2 \circ \sigma_1^{-1}}_{Aut_K(L)}(\underbrace{l_1}_{Z_L(k(t))}) = \underbrace{l_2}_{Z_L(k(t))}$, so the action is transitive

Date / /

(c) Definition: Let $K \subseteq L$ be a field extension.

If $|Aut_K(L)| = [L:K] < +\infty$, then $K \subseteq L$ is Galois.

(d) Proposition: Let $K \subseteq M$ be a field extension.

If H is a subgroups of $Aut(M/K)$,

then $L = M^H$ is a subfield of M containing K.

M	$\{e\}$
$\cup$	$\cap$
L	H
$\cup$	$\cap$
K	$Aut(M/K)$

Proof: We may divide our proof into four steps.

Step1: $0 \in K \Rightarrow \forall \sigma \in H, \sigma(0) = 0 \Rightarrow 0 \in L = M^H$

$1 \in K \Rightarrow \forall \sigma \in H, \sigma(1) = 1 \Rightarrow 1 \in L = M^H$

Step2: $k_1, k_2 \in L = M^H \Rightarrow \forall \sigma \in H, \sigma(k_1) = k_1, \sigma(k_2) = k_2$

$\Rightarrow \forall \sigma \in H, \sigma(k_1 + k_2) = k_1 + k_2 \Rightarrow k_1 + k_2 \in L = M^H$

$k_1, k_2 \in L = M^H \Rightarrow \forall \sigma \in H, \sigma(k_1) = k_1, \sigma(k_2) = k_2$

$\Rightarrow \forall \sigma \in H, \sigma(k_1 k_2) = k_1 k_2 \Rightarrow k_1 k_2 \in L = M^H$

Step3: $k \in L = M^H \Rightarrow \forall \sigma \in H, \sigma(k) = k$

$\Rightarrow \forall \sigma \in H, \sigma(-k) = -k \Rightarrow -k \in L = M^H$

$k \in L^\times = (M^H)^\times \Rightarrow \forall \sigma \in H, \sigma(k) = k$

$\Rightarrow \forall \sigma \in H, \sigma(\frac{1}{k}) = \frac{1}{k} \Rightarrow \frac{1}{k} \in L = M^H$

Step4: $k \in K \Rightarrow \forall \sigma \in H, \sigma(k) = k \Rightarrow k \in L = M^H$.

Proposition: Let $K \subseteq M$ be a field extension.

If L is a subfield of M containing K,

then $H = Aut(M/L)$ is a subgroup of $Aut(M/K)$

M	$\{e\}$
$\cup$	$\cap$
L	H
$\cup$	$\cap$
K	$Aut(M/K)$

Proof: We may divide our proof into three steps.

Step1: $\forall l \in L, id_M(l) = l \Rightarrow id_M \in Aut(M/L)$

Step2: $\sigma, \tau \in Aut(M/L) \Rightarrow \forall l \in L, \sigma(l) = \tau(l) = l$

$\Rightarrow \forall l \in L, \sigma\tau(l) = l \Rightarrow \sigma\tau \in Aut(M/L)$

Step3: $\sigma \in Aut(M/L) \Rightarrow \forall l \in L, \sigma(l) = l$

$\Rightarrow \forall l \in L, \sigma^{-1}(l) = l \Rightarrow \sigma^{-1} \in Aut(M/L)$

Date / /

Theorem: Let L be a field, and H be a finite subgroup of $\mathrm{Aut}(L)$.
$L^H \subseteq L$ is a Galois extension, and $\mathrm{Aut}_{L^H}(L) = H$.

Proof: We may divide our proof into three steps.

Step1: We prove that $L^H \subseteq L$ is separable.

For all $\alpha_1 \in L$, $H*\alpha_1$ is finite.
Assume that $H*\alpha_1$ consists of distinct elements $\alpha_1, \alpha_2, \cdots, \alpha_n$.
According to Vieta's theorem, $f(x) = \prod_{k=1}^{n}(x-\alpha_k) = \sum_{l=0}^{n}(-1)^{n-l}x^l$
$\sum_{k_1,k_2,\cdots,k_{n-l}} \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_{n-l}} \in L^H[x]$ completely splits into distinct linear factors, including $x-\alpha_1$, over L, so $f(x) \in L^H[x]$ is separable, $\alpha_1 \in L$ is separable over L^H, $L^H \subseteq L$ is separable.

Step2: We prove that $L^H \subseteq L$ is normal.

First, for all $\alpha_1 \in L$, $L^H(\alpha_1)$ is an intermediate field between L^H and L, satisfying $[L^H(\alpha_1) : L^H]$ = The degree of the minimal polynomial of α_1 over $L^H \le \deg \prod_{k=1}^{n}(x-\alpha_k) = |H*\alpha_1| \le |H|$,
so there exists $\alpha_i \in L$, such that $[L^H(\alpha_i) : L^H]$ is maximal.

Second, for all $\beta \in L$, $L^H(\alpha_i, \beta)$ is a finite separable extension of L^H, so for some $\alpha_n \in L$, $\beta \in L^H(\alpha_i, \beta) = L^H(\alpha_n) \subseteq L^H(\alpha_i)$.
This implies $L = L^H(\alpha_i)$ is the splitting field of $\prod_{k=1}^{n}(x-\alpha_k)$ over L^H,
so $L^H \subseteq L$ is normal.

Date / /

Step3: We prove that $Aut_{L^H}(L)=H$.

$L=L^H(\alpha_1)$ is a simple extension of L^H, and $\prod_{k=1}^{n}(x-\alpha_k)\in L^H[x]$ is the minimal polynomial of α_1 over K for degree reason, and $\{\alpha_1,\cdots,\alpha_n\}$ is the set of roots of $\prod_{k=1}^{n}(x-\alpha_k)$ on L. According to (b):

$$|Aut_{L^H}(L)|=|\{\alpha_1,\cdots,\alpha_n\}|=|H|.$$

As $H\le Aut_{L^H}(L)$, we may conclude that $H=Aut_{L^H}(L)$

(c) Proof: We may divide our proof into two parts.

"if" direction: Assume that $L^G=K$.

Now $K=L^G\le L$ is Galois, and $Aut_{L^G}(L)=G$.

"only if" direction: Assume that $K\le L$ is Galois and $G=Aut_K(L)$.

For all $\alpha\in L\setminus K$, consider the minimal polynomial $f(x)$ of α over K. As $K\le L$ is Galois, $f(x)$ completely splits into distinct linear factors in L, so we may choose $\beta\in L\setminus(K\cup\{\alpha\})$, and conclude that α is not fixed under some automorphism of L fixing K while sending α to β. This implies $\alpha\in L\setminus L^G$.

(8) Proof: Splitting field $\Rightarrow$ Normal extension of K; Characteristic $0\Rightarrow$ Separable extension of K $\Rightarrow$ Galois extension of K.

(9) Proof: $Gal(\mathbb{Q}[\zeta_n]/\mathbb{Q})=Gal(\mathbb{Q}[\zeta_n]/\mathbb{Q}[\zeta_n]^{\mathbb{Z}_n^\times})=\mathbb{Z}_n^\times$

Here, $\mathbb{Z}_n^\times$ contains all field automorphism of $\mathbb{Q}[\zeta_n]$ sending ζ_n to ζ_n^k, where $(k,n)=1$.

(10) Proof: $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^n}^{\mathbb{Z}/n}) = \mathbb{Z}/n$

Here, $\mathbb{Z}/n$ contains all powers of the Frobenius automorphism.

(11) Proof: Forall $\sigma \in Aut_K(L)$, forall $\alpha \in M$, $\sigma(\alpha) = \beta \in L$

Assume that the minimal polynomial of α over K is $f_K(x)$.

As $\sigma|_K = id_K$, $f_K(\beta) = f_K \circ \sigma(\alpha) = \sigma \circ f_K(\alpha) = \sigma(0) = 0$

According to the definition of splitting field, $\beta \in M$.

(12) Theorem: Let $K \subseteq L$ be a (finite) Galois extension.

(i) For all intermediate field $K \subseteq M \subseteq L$, $M \subseteq L$ is Galois.

(ii) The two maps below are inverses to each other.

$$\begin{array}{ccc} L & & \{e\} \\ \cup & & \cap \\ M & \xrightarrow{H = Aut_M(L)} & H \\ \cup & \xleftarrow{M = L^H} & \cap \\ K & & G \end{array}$$

Proof: We may divide our proof into three steps.

Step 1: $K \subseteq L$ is Galois $\Rightarrow$ L is the splitting field of some separable $f(x) \in K[x]$

$\Rightarrow$ L is the splitting field of some separable $f(x) \in M[x] \Rightarrow M \subseteq L$ is Galois.

Step 2: According to Artin's theorem, $Aut_{L^H}(L) = H$

Step 3: As $M \subseteq L$ is Galois, $L^{Aut_M(L)} = M$

(13) Every intermediate field $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$ is in the form $\mathbb{F}_{p^d}$, where $d|n$.

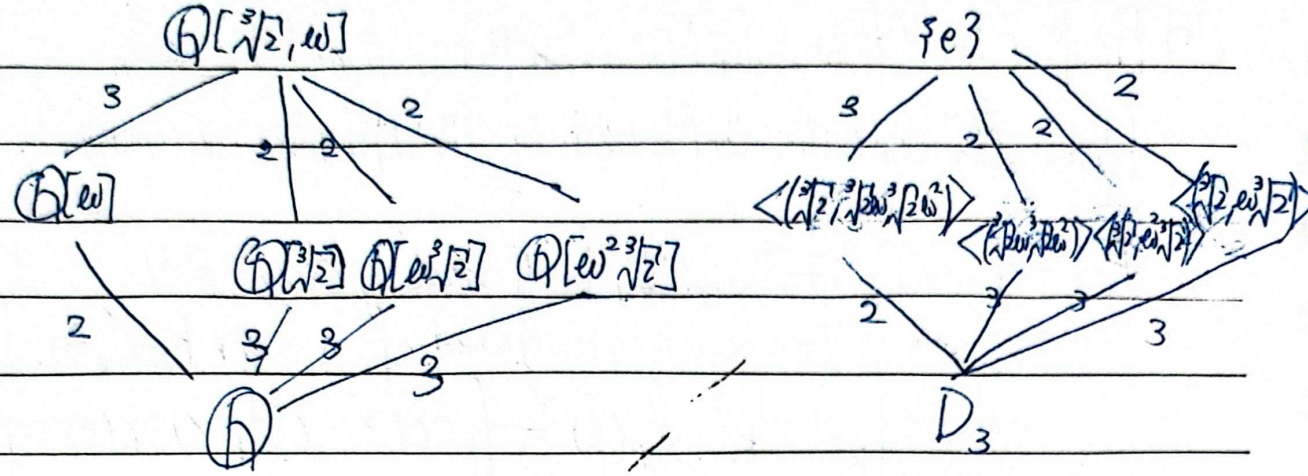
Every subgroup H of $\mathbb{Z}/n$ is in the form $\mathbb{Z}/d$, where $d|n$.

In this case, $Aut_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^n}) = \{(x \mapsto x^{p^k}) : d | k\} = \mathbb{Z}/n/d$

$$\mathbb{F}_{p^n}^{\mathbb{Z}/d} = \{x : x^{p^d} - x = 0\} = \mathbb{F}_{p^{n/d}}$$

Date

(14)



(15) Proof: First, $\prod_{k=1}^{r}(x-\alpha_k) = \sum_{n=0}^{r} x^n (-1)^{r-n} \sum_{k_1,k_2,\cdots,k_{r-n}} \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_{r-n}} \in L^{G}_{[x]} = K[x]$,

has a root $\alpha_1 \in L$, so the minimal polynomial of α_1 over K divides $\prod_{k=1}^{r}(x-\alpha_k)$

Second, the minimal polynomial of α_1 over K has at least $r = |G * \alpha_1|$

roots, so it is $\prod_{k=1}^{r}(x-\alpha_k)$

(16)

(a) $L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ is the splitting field of $x^4 - 7x^2 + 10 \in \mathbb{Q}[x]$,

so $L_1/\mathbb{Q}$ is Galois.

(b) $L_2 = \mathbb{Q}(e^{2\pi i/9})$ is the splitting field of $\Phi_9(x) \in \mathbb{Q}[x]$,

so $L_2/\mathbb{Q}$ is Galois.

(c) There exists a polynomial $x^9 - 2$ in $\mathbb{Q}[x]$, such that $x^9 - 2$

has a root $\sqrt[9]{2}$, but doesn't split into linear factors, over $\mathbb{Q}[\sqrt[9]{2}]$,

so $L_3/\mathbb{Q}$ is not Galois.

(d) Assume to the contrary that $\mathbb{Q}[\sqrt{3+\sqrt{7}}]/\mathbb{Q}$ is Galois,

so $f(x)=(x-\sqrt{3+\sqrt{7}})(x-\sqrt{3-\sqrt{7}})(x+\sqrt{3+\sqrt{7}})(x+\sqrt{3-\sqrt{7}})$

$=x^4-6x^2+2\in\mathbb{Q}[x]$ completely splits over $\mathbb{Q}[\sqrt{3+\sqrt{7}}]$.

On one hand, $2\nmid 1, 2\mid 0, 2\mid(-6), 2\mid 0, 2\mid 2, 2^2\nmid 2$, $f(x)$ is irreducible over $\mathbb{Q}$,

$f(x)$ is indeed the minimal polynomial of $\sqrt{3+\sqrt{7}}$, $[\mathbb{Q}[\sqrt{3+\sqrt{7}}]:\mathbb{Q}]=4$.

On the other hand, $\sqrt{7}=(\sqrt{3+\sqrt{7}})^2-3\in\mathbb{Q}[\sqrt{3+\sqrt{7}}]$, $\sqrt{2}=\sqrt{3+\sqrt{7}}\sqrt{3-\sqrt{7}}$

$\in\mathbb{Q}[\sqrt{3+\sqrt{7}}]$, the intermediate extension $\mathbb{Q}\subseteq\mathbb{Q}[\sqrt{2},\sqrt{7}]\subseteq\mathbb{Q}[\sqrt{3+\sqrt{7}}]$

satisfies $[\mathbb{Q}[\sqrt{2},\sqrt{7}]:\mathbb{Q}]=[\mathbb{Q}[\sqrt{3+\sqrt{7}}]:\mathbb{Q}]=4$, so $\mathbb{Q}[\sqrt{2},\sqrt{7}]=\mathbb{Q}[\sqrt{3+\sqrt{7}}]$.

Now for some $a,b,c,d\in\mathbb{Q}$, $\sqrt{3+\sqrt{7}}=a+b\sqrt{2}+c\sqrt{7}+d\sqrt{14}$.

Date / /

$$\begin{cases} 3 = a^2 + 2b^2 + 7c^2 + 14d^2 & ① \\ 0 = 2ab + 14cd & ② \\ 1 = 2ac + 4bd & ③ \\ 0 = 2ad + 2bc & ④. \end{cases}$$

From ②, ④, we may deduce:

$$ab + 7cd = 0, \quad abd + 7cd^2 = 0, \quad -b^2c + 7cd^2 = 0,$$

Case 1: If $c = 0$, then:

$$ab = 0$$
$$4bd = 1$$
$$ad = 0$$

so $a = 0$, $2b^2 + 14d^2 = 3 = 12bd$, $b^2 - 6bd + 7d^2 = 0$.

$\Delta = (-6)^2 - 4 \cdot 1 \cdot 7 = 36 - 28 = 8$ is not a perfect square,

so $b = d = 0$, which leads to a contradiction $0 = 4bd = 1$.

Case 2: If $b^2 - 7d^2 \neq 0$ then $\Delta = 0^2 - 4 \cdot 1 \cdot (-7) = 28$ is not a perfect square,

which implies $b = d = 0$, now $a^2 + 7c^2 = 3 = 6ac$, $a^2 - 6ac + 7c^2 = 0$,

similar argument leads to a contradiction.

Hence, ④ $\mathbb{Q}[\sqrt{3+\sqrt{7}}]/\mathbb{Q}$ is not Galois.