1 Introduction to Galois theory assignmens 2, Problem 1

Let $F = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/9}$.

Problem 1.1 *What is the degree $[F : \mathbb{Q}]$? Recall why F is a Galois extension of $\mathbb{Q}$. What is the Galois group of F over $\mathbb{Q}$?*

Solution: From $\phi_9 = P_9/(\phi_1 \cdot \phi_3) = X^6 + X^3 + 1$, we know $[F : \mathbb{Q}] = 6$. Because it's splitting field fo P_9, hence must be Galois. By cyclotomic extension theorem,

$$Gal(F/\mathbb{Q}) \simeq (\mathbb{Z}/9\mathbb{Z})^*$$

. ☐

Problem 1.2 *Let $\alpha = \cos(2\pi/9)$. Find the minimal polynomial of ζ over $\mathbb{Q}(\alpha)$ and show that $\mathbb{Q}(\alpha) = F \cap \mathbb{R}$.*

Solution: From $\alpha = \zeta + \bar{\zeta} = \zeta + \zeta^{-1}$, we have minimal polynomial is $X^2 - \alpha X + 1$, the Galois group is generated by conjugation, hence $\mathbb{Q}(\alpha) = F^{Gal(F/\mathbb{Q}(\alpha))} = F \cap \mathbb{R}$. ☐

Let γ stand for the (real) 9th root of 5(i.e. $\gamma = \sqrt[9]{5}$), M for the splitting field $X^9 - 5$, and L for $\mathbb{Q}(\gamma)$.

Problem 1.3 *What is the degree $[L : \mathbb{Q}]$? Let K be a subfield of L, not equal to L or $\mathbb{Q}$. What can one say about the degree $[L : K]$? Prove that $K = \mathbb{Q}(\gamma^3)$ (hint: consider the minimal polynomial of γ over K).*

Solution: $X^9 - 5$ is irreducible, hence $[L : \mathbb{Q}] = 9$. Because $[L : K] | [L : \mathbb{Q}]$, it has to be 3.

$P_{\min}(\gamma, K) | X^9 - 5$, hence it must be as following:

$$X^3 - \gamma(\zeta^a + \zeta^b + \zeta^c)X^2 + \gamma^2(\zeta^{a+b} + \zeta^{b+c} + \zeta^{c+a})X - \gamma^3\zeta^{a+b+c}$$

However, L is real, hence K is real, only possible way is $a = 0, b = 3, c = 6$, i.e. $X^3 - \gamma^3$, hence $K = \mathbb{Q}(\gamma^3)$.

☐

Problem 1.4 *Compute $F \cap L$, then $[M : \mathbb{Q}]$.*

Solution: $F \cap L \subset F \cap \mathbb{R} = \mathbb{Q}(\alpha)$, however $L/\mathbb{Q}$ can't have sub-extension of order 2, hence $F \cap L = \mathbb{Q}$.(because $\alpha \notin L$).

Hence they are linear disjoint over $F \cap L = \mathbb{Q}$, then $[M : \mathbb{Q}] = 54$. ☐

Problem 1.5 *Show that $G = Gal(M/\mathbb{Q})$ has a cyclic normal subgroup H of 9 elements, and also a cyclic subgroup S which is isomorphic to G/H under the projection map. Is G commutative?*

Solution: Let σ be the generator of H, where

$$\sigma : \gamma \mapsto \gamma \cdot \zeta$$

it's well defined, and cyclic of order 9. And $M^H = \mathbb{Q}(\zeta)$ which is normal, hence H is normal.

Let S be generated by following:

$$\tau : \zeta \mapsto \zeta^2$$

hence $S \simeq (\mathbb{Z}/9\mathbb{Z})^*$, if we restrice G on μ_9^*, we have $H \subset \mathrm{Ker}(G \to \mu_9^*)$, but $|G| = 54$, and $|H| = 9$ and $|S| = 6$, it must be the following exact sequence.

$$1 \to H \to G \to S \to 1$$

It's easy to see $\sigma\tau \neq \tau\sigma$, hence not abelian.

□

Problem 1.6 *Describe all subextensions of M which are of degree 2 over $\mathbb{Q}$.*

Solution: Let the subextension be N, where $\mathbb{Q} \hookrightarrow N \hookrightarrow M$, and $[N : \mathbb{Q}] = 2$. Because the degree over $\mathbb{Q}$ is 2, it must be galois over $\mathbb{Q}$. Hence its corresponding group is of order 27.

By Sylow theorem the 3-sylow group of $Gal(M/\mathbb{Q})$ is of order 27, and the number of such 3-sylow groups (call it r) must divide $|Gal(M/\mathbb{Q})|$, and $r \mod 3 = 1$, it can only be $r = 1$. Hence there is an unique subextension of degree 2.

Consider $\omega = \zeta^3 = e^{2\pi i/3}$, we have $\tau^2(\omega) = \omega$, hence $\mathbb{Q}(\omega)$ is the only subextensions of order 2. □

Problem 1.7 *Describe all Galois subextensions of M which are of degree 3 over $\mathbb{Q}$.*

Solution: It's easy to verify $\tau^3(\alpha) = 1$, hence $\mathbb{Q}(\alpha)$ is a galois extension of order 3.

Should only be this one. □

2 Introduction to Galois theory assignmens 2, Problem 2

Let k be a field of characteristic $p > 0$, $0 \neq a \in k$, $P = X^p - aX - b \in k[X]$, K splitting field of P.

Problem 2.1 *Why is K a Galois extension of k? Show that $X^{p-1} - a$ is split over K and its roots together with 0 form a subgroup of K, isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Solution: Obviously by differential it's separable, hence must be galois.

Let x be a root of P and y be a root $X^{p-1}-a$, then by Frobenious mapping:

$$(x+y)^p - a(x+y) - b = P(x) - y(y^{p-1}-a) = y(y^{p-1}-a) = 0$$

So $x+y_i$ where y_i are all roots of $X^{p-1}-a$ are roots of P, because P split, hence $X^{p-1}-a$ must split.(Because $x+y_i \in K$ and $x \in K$)

Because any y_i or 0 induce the following mapping:

$$y_i : x \mapsto x + y_i$$

which is an element of $Gal(K/k)$, it forms a group, and of order p, which is prime, must be cyclic. □

Problem 2.2 *What do we know about the Galois group of the splitting field L of the polynomial $X^{p-1}-a$ over k?*

Solution: It's subfield of K. □

Problem 2.3 *Let $G = Gal(K/k)$, $H = Gal(K/L)$. Show that for any $g \in G$ and x a root of P, $gx - x$ is either zero or a root of $X^{p-1}-a$; moreover for $g \in H$ this element does not depend on x.*

Solution:

$$\begin{aligned}0 &= g(x^p - ax - b) - (x^p - ax - b) = g(x)^p - ag(x) - b - x^p + ax + b \\ &= g(x)^p - x^p - a(g(x) - x) = (gx - x)^p - a(gx - x) \\ &= (gx - x)((gx - x)^{p-1} - a)\end{aligned}$$

hence $gx - x = 0$ or $gx - x$ is a root of $X^{p-1}-a$.

All roots of P can be written as $x + y_i$, hence $g(x+y_i) - (x+y_i) = gx - x$ for $g \in Gal(K/L)$, hence independent on x.

□

Problem 2.4 *Show that H has either 1 or p elements.*

Solution: From 2.3, we have map

$$h \mapsto hx - x$$

whose images are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Hence must to either trivial or full. □

Problem 2.5 *Prove the equivalence of the following three properties:*

1. *$H = \mathbb{Z}/p\mathbb{Z}$*
2. *P is irreducible over L*
3. *P is irreducible over k*

Solution: $1 \to 2$, P is splitting, have to be irreducible, or the degree less than p.

$2 \to 3$, by 2.1, all $Gal(K/k)$ have already p elements, P have to be irreducible.

$3 \to 1$, by 2.4, if not, then $K = L$, impossible for P to be irreducible because $[L : k] \leq p - 1$. $\square$

Problem 2.6 *Let $k = \mathbb{F}_p(T)$ (the field of rational functions in one variable and coefficients in $\mathbb{F}_p$). What is the order of the Galois group of $P(X) = X^p - TX - T$?*

Solution: Let $L = k(\sqrt[p-1]{T})$, and P is irreducible over $\mathbb{F}_p[T]$, hence $[K : L] = p$. Hence the order is $p(p-1)$.

$\square$