NAP 2018 Module-V: Applications of Galois theory Solutions of Problem set 1

(1) (i) Let $\alpha = \sqrt[3]{2}$ and ω be a cube root of unity. Prove that $\alpha + \omega$ is a primitive element of $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$.
(ii) For the field extension $\mathbb{F}_8/\mathbb{F}_2$ find a primitive element.
(iii) For a prime number p, find the number of intermediate fields for the extension $\mathbb{F}_{p^{12}}/\mathbb{F}_p$. How many of them are proper, i.e. different from $\mathbb{F}_p$ and $\mathbb{F}_{p^{12}}$?

Solution: (i) Let $L = \mathbb{Q}(\alpha + \omega)$. Since $(\alpha + \omega)^3 = 3 + 3\alpha\omega(\alpha + \omega)$, $\alpha\omega \in L$. Thus $\alpha^2 + \omega^2 = (\alpha + \omega)^2 - 4\alpha\omega \in L$ which implies that $\alpha\omega(\alpha^2 + \omega^2) = \alpha^3\omega + \alpha\omega^3 = 2\omega + \alpha \in L$. Therefore $\omega = 2\omega + \alpha - (\alpha + \omega) \in L$ and hence $\alpha \in L$. Therefore $L = \mathbb{Q}(\alpha + \omega)$.

OR

We know that $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ where

$$\begin{array}{lllllllllll} \sigma_1: & \alpha \mapsto \alpha & \sigma_2: & \alpha \mapsto \alpha\omega & \sigma_3: & \alpha \mapsto \alpha\omega & \sigma_4: & \alpha \mapsto \alpha\omega^2 & \sigma_5: & \alpha \mapsto \alpha\omega^2 \\ & \omega \mapsto \omega^2 & & \omega \mapsto \omega & & \omega \mapsto \omega^2 & & \omega \mapsto \omega & & \omega \mapsto \omega^2. \end{array}$$

Since $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ and α is real, it can be verified that $\sigma_i(\alpha + \omega) \neq \alpha + \omega$ for any $i = 1, \ldots, 5$. Therefore $\alpha + \omega$ is a primitive element.

(ii) Write $\mathbb{F}_8 \cong \mathbb{F}_2[X]/(f(X))$ for some irreducible polynomial $f(X)$ of degree 3 in $\mathbb{F}_2[X]$. (Only irreducible polynomials of degree 3 in $\mathbb{F}_2[X]$ are $X^3 + X + 1$ and $X^3 + X^2 + 1$). Let $\overline{x}$ denote the image of x in $\mathbb{F}_2[X]/(f(X))$. Then $\overline{x}$ is a primitive element for $\mathbb{F}_8/\mathbb{F}_2$.

(iii) We know that $\mathbb{F}_{p^{12}}/\mathbb{F}_p$ is Galois with Galois group $\mathbb{Z}/12\mathbb{Z}$. By Fundamental theorem of Galois theory we know that the number of intermediate fields for the extension $\mathbb{F}_{p^{12}}/\mathbb{F}_p$ is equal to the number of subgroups of the Galois group (which in this case is $\mathbb{Z}/12\mathbb{Z}$). Since $\mathbb{Z}/12\mathbb{Z}$ is cyclic, for each divisor d of 12 there exists a unique subgroup of order d. Therefore the number of subgroups is equal to the number of divisors of 12 which is equal to 6.

Moreover, the intermediate field is proper if and only if the subgroup of $\mathbb{Z}/12\mathbb{Z}$ is proper. Hence the number of proper intermediate fields is 4.

(2) For a prime number p let $\mathbb{F}_p$ be the field with p elements. Let $E = \mathbb{F}_p(X, Y)$ and $F = \mathbb{F}_p(X^p, Y^p)$. Consider the field extension E/F. Prove that there exist infinitely many intermediate fields. (Warning: $\mathbb{F}_p$ is not algebraically closed.)
Solution: Let $F = \mathbb{F}_p(X^p, Y^p)$. For $c \in F$, consider the intermediate fields $F(X + cY)$. We claim that if $c \neq c' \in F$, then $F(X + cY) \neq F(X + c'Y)$. Suppose $F(X + cY) = F(X + c'Y)$. Then $X, Y \in F(X + cY)$ and hence $F(X + cY) = F(X, Y)$. But $(X + cY)^p = X^p + c^pY^p \in F$ and hence $[F(X, Y) : F] \leq p$. This is a contradiction as $[F(X, Y) : F] = p^2$.

Thus for each $c \in F$ we get distinct intermediate fields. Since F is infinite, the number of intermediate fields is infinite.

(3) Let ζ be the primitive 9-th roots of unity in $\mathbb{C}$.
(i) Verify that $\Phi_9(X) = \Phi_3(X^3)$.
(ii) Find the irreducible polynomial for ζ over $\mathbb{Q}$.
(iii) Determine the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Solution: (i) We have

$$\begin{aligned}\Phi_3(X) &= \frac{X^3-1}{\Phi_1(X)} = \frac{X^3-1}{X-1} = X^2+X+1\\ \Phi_9(X) &= \frac{X^9-1}{\Phi_1(X)\Phi_3(X)} = \frac{X^9-1}{X^3-1} = X^6+X^3+1.\end{aligned}$$

Hence $\Phi_9(X) = \Phi_3(X^3)$.
(ii) We know that $\Phi_n(X)$ is the minimal polynomial for a primitive n-th root of unity over $\mathbb{Q}$. Thus

$$\mathrm{irr}(\zeta;\mathbb{Q}) = \Phi_9(X) = X^6+X^3+1.$$

(iii) We know that for a primitive n-th root of unity ζ, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}.$$

(4) Consider the Galois extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ and the norm map N. For $a,b,c,d \in \mathbb{Q}$, find $N(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)$.
Solution: Recall the definition of the norm map for the Galois extension E/F, $N : E \to F$ is given by

$$N(x) = \prod_{\sigma\in G} \sigma(x).$$

The degree of the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is 4 and the Galois group for this extension

$$G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

We write $G = \{id,\sigma,\tau,\sigma\tau\}$ where id is the identity element and

$$\begin{aligned}\sigma(\sqrt{2}) = -\sqrt{2} \text{ and } \sigma(\sqrt{3}) = \sqrt{3} (\Rightarrow \sigma(\sqrt{6}) = -\sqrt{6})\\ \tau(\sqrt{2}) = \sqrt{2} \text{ and } \tau(\sqrt{3}) = -\sqrt{3} (\Rightarrow \tau(\sqrt{6}) = -\sqrt{6})\\ \sigma\tau(\sqrt{2}) = -\sqrt{2} \text{ and } \sigma\tau(\sqrt{3}) = -\sqrt{3} (\Rightarrow \sigma\tau(\sqrt{6}) = \sqrt{6}.\end{aligned}$$

Then

$$\begin{aligned}& N(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\\ =\ & id(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\cdot\sigma(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\\ & \cdot\tau(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\cdot\sigma\tau(a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\\ =\ & (a+\sqrt{2}b+\sqrt{3}c+\sqrt{6}d)\cdot(a-\sqrt{2}b+\sqrt{3}c-\sqrt{6}d)\\ & \cdot(a+\sqrt{2}b-\sqrt{3}c-\sqrt{6}d)\cdot(a-\sqrt{2}b-\sqrt{3}c+\sqrt{6}d)\\ =\ & (a^2-2b^2+3c^2-6d^2)^2-12(ac-2bd)^2\\ =\ & (a^4+4b^4+9c^4+36d^4-4a^2b^2+6a^2c^2-12a^2d^2-12b^2c^2+24b^2d^2-36c^2d^2)\\ & -12(a^2c^2+4b^2d^2-4abcd)\\ =\ & a^4+4b^4+9c^4+36d^4-4a^2b^2-6a^2c^2-12a^2d^2-12b^2c^2-24b^2d^2-36c^2d^2-48abcd.\end{aligned}$$

(5) Let $d > 0$ be a square-free integer (or rational number). For the quadratic field extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ verify the Hilbert's Theorem 90. In other words, for $a, b \in \mathbb{Q}$ with $N(a + b\sqrt{d}) = a^2 - db^2 = 1$ find $x, y \in \mathbb{Q}$ such that

$$a + b\sqrt{d} = \frac{x + y\sqrt{d}}{x - y\sqrt{d}}.$$

Solution: Let $a, b \in \mathbb{Q}$ be such that $N(a + b\sqrt{d}) = a^2 - db^2 = 1$. Write $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{id, \sigma\}$. Note that $\sigma(\sqrt{d}) = -\sqrt{d}$.

Case 1: $b = 0$. Then $N(a) = a^2 = 1 \Rightarrow a = \pm 1$. If $a = 1$ take $x = 1$ and $y = 0$. If $a = -1$ take $x = 0$ and $y = 1$.

Case 2: $b \neq 0$. [Note that in this case $a \neq \pm 1$ because if $a = 1$ then $a^2 - db^2 = 1 \Rightarrow db^2 = 0 \Rightarrow b = 0$.] We want to solve $a + b\sqrt{d} = \frac{x+y\sqrt{d}}{x-y\sqrt{d}}$ for $x, y \in \mathbb{Q}$. We get system of equations

$$\begin{aligned} (1 - a)x + bdy &= 0 \\ bx - (1 + a)y &= 0 \end{aligned}$$

Since $a^2 - db^2 = 1$ the discriminant is equal to $a^2 - 1 - db^2 = 0$. So the system has infinitely many solutions. We can take $x = 1$ and $y = \frac{a-1}{bd}$. Then verify

$$a + b\sqrt{d} = \frac{1 + \frac{a-1}{bd}\sqrt{d}}{1 + \frac{a-1}{bd}\sqrt{d}}.$$