Solution 25

Galois correspondence. Solvability by radicals.

1. In class, we stated the following result:

   Proposition. Let k be a field of characteristic 0 and E/k a finite Galois extension with solvable $\mathrm{Gal}(E/k)$. Then E is contained in a radical extension of k.

   In order to prove this result, we do an induction on $|\,\mathrm{Gal}(E/k)| = [E : k]$. In the case $E \neq k$ we take a normal subgroup $N \lhd \mathrm{Gal}(E/k)$ of prime index p (using Assignment 21, Exercise 3) and define k^* as the splitting field of $X^p - 1 \in k[X]$.

   (a) Prove that $k^* = k(w)$ for some root w of $X^p - 1 \in k[X]$. Define $E^* := E(w)$.

   (b) Assume that $k^* = k$. Prove that E^N/k is a pure extension and conclude.

   (c) Suppose now that $k^* \neq k$. Show that E^*/k^* is a Galois extension and that $\mathrm{Gal}(E^*/k^*)$ injects into $\mathrm{Gal}(E/k)$.

   (d) Deduce that $\mathrm{Gal}(E^*/k^*)$ is solvable and that E^*/k^* is contained in a radical field extension M/k^*.

   (e) Explain why M/k is radical as well and conclude the proof of the Lemma.

   Solution:

   (a) This is clear, because the p-th roots of 1 are all powers of a given non-trivial one.

   (b) We know that $[E^N : k] = [G : N] = p$ and that k contains all p-th roots of 1. Then we can apply Corollary IV.24 and obtain that $E^N = k(u)$ for some $u \in E^N$ such that $u^p \in k$. Hence E^N/k is a pure extension. Moreover, the extension E/E^N is contained in a radical one by inductive hypothesis, as

   $$[E : E^N] = \frac{[E : k]}{p} < [E : k]$$

   and the subgroup $\mathrm{Gal}(E/E^N)$ of the solvable group $\mathrm{Gal}(E/k)$ is solvable by Proposition III.17. Hence E/k is contained in a radical extension.

   (c) Write $E = \mathrm{Sf}(f)$ for some $f \in k[X]$. Since $E^* = E(w)$, we know that $E^* = \mathrm{Sf}((X^p - 1)f)$ is a Galois extension of k and hence a Galois extension of k^*. We are then in position of using Assignment 19, Exercise 3 to conclude that there exists an injective group homomorphism $\mathrm{Gal}(E^*/k^*) \longrightarrow \mathrm{Gal}(E/k)$ given by restriction of automorphisms.

(d) $\mathrm{Gal}(E^*/k^*)$ is isomorphic to a subgroup of $\mathrm{Gal}(E/k)$. This subgroup is solvable by Proposition III.17. Hence $\mathrm{Gal}(E^*/k^*)$ is solvable as well. The proof in the case in which the base field contains non-trivial p-th roots of 1 was done in (a), so that E^*/k^* is contained in a radical extension M/k^*.

(e) The extension k^*/k is pure by definition. Hence M/k is radical. Since it contains E/k, we are done.

2. Let p be an odd prime number. Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{F}_p^\times$. For $a \in \mathbb{F}_p^\times$, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } a \text{ is a not square in } \mathbb{F}_p^\times. \end{cases}$$

Define the complex number

$$\tau = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a.$$

(a) Show that the map $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ sending $a \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism.

(b) Prove that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p),$$

and that this determines $\left(\frac{a}{p}\right) \in \{\pm 1\}$ uniquely.

(c) Show that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.

(d) For $b \in \mathbb{F}_p^\times$, let $\sigma_b \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism $\sigma_b(\zeta) = \zeta^b$. Prove the equality $\sigma_b(\tau) = \left(\frac{b}{p}\right) \cdot \tau$.

(e) Prove that $\mathbb{Q}(\tau)/\mathbb{Q}$ is the unique quadratic intermediate extension of $E/\mathbb{Q}$.

We now want to determine the extension $\mathbb{Q}(\tau)$ by computing τ^2 explicitly.

(f) Let $c \in \mathbb{F}_p^\times$. Show that

$$\sum_{a \in \mathbb{F}_p^\times} \zeta^{a(1+c)} = \begin{cases} -1 & \text{if } c \neq p-1 \\ p-1 & \text{if } c = p-1 \end{cases}$$

(g) Write

$$\tau^2 = \sum_{a \in \mathbb{F}_p^\times} \sum_{b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Substituting $b = ac$ with $c \in \mathbb{F}_p^\times$, deduce that

$$\tau^2 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1).$$

(h) Conclude: if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$; if $p \equiv 3 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$.

Solution:

(a) The group $\mathbb{F}_p^\times$ is cyclic of even order $p-1$. Since it is abelian, the map $s : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ sending $x \mapsto x^2$ is a group homomorphism. The set of squares in $\mathbb{F}_p^\times$ is given by $S = \{s(x),\, x \in \mathbb{F}_p^\times\} = \mathrm{im}(s)$. By the First Isomorphism Theorem, s induces an isomorphism $\mathbb{F}_p^\times / \ker(s) \xrightarrow{\sim} S$. Moreover $\ker(s) = \{x \in \mathbb{F}_p^\times : x^2 = 1\} = \{\pm 1\}$ because it contains the roots of the degree-2 polynomial $X^2 - 1 \in \mathbb{F}_p[X]$. Hence S is a subgroup of order 2 of $\mathbb{F}_p^\times$, implying that for $a, b \in \mathbb{F}_p^\times$ the element $ab \in \mathbb{F}_p^\times$ is a square if and only if a and b are both square or both are not squares. In particular, the given map is a group homomorphism.

(b) The group $\mathbb{F}_p^\times$ is the set of roots of $X^{p-1} - 1 \in \mathbb{F}_p[X]$. Since $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$, we know that precisely $\frac{p-1}{2}$ elements in $a \in \mathbb{F}_p^\times$ satisfy $a^{\frac{p-1}{2}} = 1$, the others satisfying $a^{\frac{p-1}{2}} = -1$. If $a = b^2$ for $b \in \mathbb{F}_p^\times$, then $a^{\frac{p-1}{2}} = b^{2 \cdot \frac{p-1}{2}} = 1$. Since by part (a) there are precisely $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$, we conclude that $a^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p$ when a is not a square. Hence $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ for each $a \in \mathbb{F}_p \times$.

(c) By part (b),

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

which is 1 if and only if $p-1$ is divisible by 4, that is, if and only if $p \equiv 1 \pmod 4$.

(d) The power ζ^a for $a \in \mathbb{F}_p$ is well defined, because $\zeta^{pm} = 1$ for each $m \in \mathbb{Z}$. Clearly, $\tau \in E$ by definition. For each $b \in \mathbb{F}_p^\times$, we compute

$$\begin{aligned}\sigma_b(\tau) = \sigma_b\left(\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\zeta^a\right) &= \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\sigma_b(\zeta)^a = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{b}{p}\right)\left(\frac{b}{p}\right)\left(\frac{a}{p}\right)\zeta^{ba} \\ &= \left(\frac{b}{p}\right)\sum_{a \in \mathbb{F}_p^\times} \left(\frac{ba}{p}\right)\zeta^{ba} = \left(\frac{b}{p}\right)\tau,\end{aligned}$$

in the last step having used the fact that $\{ba : a \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$ for each $b \in \mathbb{F}_p^\times$, which holds because $\mathbb{F}_p^\times$ is a group.

(e) By part (d), we see that $\sigma_b(\tau^2) = \left(\frac{b}{p}\right)^2 \tau^2 = \tau^2$ for each $b \in \mathbb{F}_p$, so that $\tau^2 \in E^{\mathrm{Gal}(E/\mathbb{Q})} = \mathbb{Q}$. Moreover, $\sigma_b(\tau) \neq \tau$ when b is not a square in $\mathbb{F}_p^\times$ (which is the case for half of the elements of $\mathbb{F}_p\times$), so that $\tau \notin \mathbb{Q}$. Hence $\mathbb{Q}(\tau)/\mathbb{Q}$ is a quadratic extension.

On the other hand, the Galois group $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{F}_p^\times$ is cyclic of even order $p-1$, so it contains precisely one subgroup of index 2 (that is, of order $\frac{p-1}{2}$). Hence, there is precisely one quadratic extension $L/\mathbb{Q}$ contained in E (that is, such that $[E : L] = \frac{p-1}{2}$), which is then given by $\mathbb{Q}(\tau)$.

(f) For $c = p - 1$, we get

$$\sum_{a\in\mathbb{F}_p^\times} \zeta^{a(1+c)} = \sum_{a\in\mathbb{F}_p^\times} \zeta^{ap} = \sum_{a\in\mathbb{F}_p^\times} (\zeta^p)^a = \sum_{a\in\mathbb{F}_p^\times} 1 = p - 1.$$

Else, $1 + c \in \mathbb{F}_p^\times$, so that $\{a(1 + c) : a \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$ and

$$\sum_{a\in\mathbb{F}_p^\times} \zeta^{a(1+c)} = \sum_{a\in\mathbb{F}_p^\times} \zeta^a = -1 + \sum_{a\in\mathbb{F}_p} \zeta^a = -1,$$

because ζ is a root of $\sum_{a=0}^{p-1} X^a = \frac{X^p-1}{X-1} \in \mathbb{Z}[X]$.

(g) Since $\{ac : c \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$, we can perform the suggested substitution, as follows:

$$\tau^2 = \sum_{a\in\mathbb{F}_p^\times}\sum_{b\in\mathbb{F}_p^\times} \left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times} \left(\frac{a(ac)}{p}\right)\zeta^{a+ac} = \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times} \left(\frac{a^2c}{p}\right)\zeta^{a(1+c)}$$

$$= \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times} \left(\frac{c}{p}\right)\zeta^{a(1+c)} = \sum_{c\in\mathbb{F}_p^\times} \left(\frac{c}{p}\right)\sum_{a\in\mathbb{F}_p^\times} \zeta^{a(1+c)} \overset{(f)}{=} \left(\frac{-1}{p}\right)(p-1) - \sum_{c=1}^{p-2}\left(\frac{c}{p}\right)$$

(h) The above sum reads

$$\tau^2 = \left(\frac{-1}{p}\right)p - \left(\frac{-1}{p}\right) - \sum_{c=1}^{p-2}\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{c\in\mathbb{F}_p^\times}\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right)p,$$

because $\left(\frac{c}{p}\right)$ attains the values 1 and -1 an equal number of times for $c \in \mathbb{F}_p^\times$.
If $p \equiv 1 \pmod 4$, then

$$\tau^2 = p,$$

so that $\tau = \pm\sqrt{p}$ and $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$ is a quadratic real extension of $\mathbb{Q}$.
Else, $p \equiv 3 \pmod 4$,

$$\tau^2 = -p,$$

so that $\tau = \pm i\sqrt{p}$ and $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$ is a quadratic imaginary extension of $\mathbb{Q}$.