2017 NAP Lecture Module III, Problem 4 Solution

H. Shiga

Important Direction. At the Mid Term Exam, you are allowed to see the "Summary"", and it is not allowed to refer anything else.

Problem III -4] = Excersise Chap. 3-2:

Let p be an odd prime, and set $\zeta = e^{2\pi i/p}$. Consider the field $E = \boldsymbol{Q}[\zeta]$. It is the splitting field of $f(X) = X^{p-1} + X^{p-2} + \cdots + 1$. So (by Thm. 3.10) $E/\boldsymbol{Q}$ is Galois.

(1) Show that $G = \mathrm{Gal}(E/\boldsymbol{Q})$ is isomorphic to (the cyclic group) $(\boldsymbol{Z}/(p\boldsymbol{Z}))^\times \cong \boldsymbol{Z}/(p-1)\boldsymbol{Z}$.

[Proof] The roots of $f(X) = 0$ is given by ζ^k $(i = 1, \cdots, p-1)$. We have a generator $\sigma = \zeta^r$ of the multiplicative group $\{\zeta^k\}$. Here we note that r is a generator of $(\boldsymbol{Z}/(p\boldsymbol{Z}))^\times = \{r, r^2, \cdots, r^{p-1}\}$. The element g of G is completely determined by the image $g(\sigma) = \zeta^{r^i}$. The correspondence $g \mapsto r^i$ gives the isomorphism between G and $(\boldsymbol{Z}/(p\boldsymbol{Z}))^\times$. Note that, for $g'(\sigma) = \zeta^{r^j}$, we have $g' \circ g(\sigma) = \zeta^{r^{(i+j)}}$.

(2) Let H be the subgroup of quadratic residues in $(\boldsymbol{Z}/(p\boldsymbol{Z}))^\times$. Set $\alpha = \sum\limits_{i \in H} \zeta^i, \beta = \sum\limits_{i \in G-H} \zeta^i$.

Show that

(a) α and β are invariant under the action of H.

[Proof] We use the same r in (1). We have $\alpha = \sum\limits_{i \in H} \zeta^i = \sum\limits_{s:\text{even}} \zeta^{r^s}$ and $\beta = \sum\limits_{i \in G-H} \zeta^i = \sum\limits_{t:\text{odd}} \zeta^{r^t}$. Take any element $h \in H$. It has an expression $h = \zeta^{r^{(2a)}}$ for some $a \in \{1, \cdots, (p-1)/2\}$. Then $h\alpha = \sum\limits_{s:\text{even}} \zeta^{r^{(s+2a)}} = \alpha$. By the same way we have $h\beta = \beta$.

(b) $\sigma\alpha = \beta, \sigma\beta = \alpha$ for any $\sigma \in G - H$.

[Proof] For any $m \in G - H$, we have an expression $m = \zeta^{r^{(2b+1)}}$. Hence $m\alpha = \sum\limits_{s:\text{even}} \zeta^{r^{(s+2b+1)}} = \beta$. By the same way we have $m\beta = \alpha$.

(c) $X^2 + X + \alpha\beta \in$ Q[X].

[Proof] By (a)(b), we have $g(\alpha\beta) = g\alpha \cdot g\beta = \alpha\beta$ for any $g \in G$. It means $\alpha\beta$ is invariant under the action of G. Namely $\alpha\beta \in \boldsymbol{Q}$.

(3) By calculating $\alpha\beta$, show that

$$E^H = \begin{cases} \boldsymbol{Q}[\sqrt{p}] & p \equiv 1 (\mathrm{mod}\ 4) \\ \boldsymbol{Q}[\sqrt{-p}] & p \equiv 3 (\mathrm{mod}\ 4) \end{cases}.$$

[Proof] First, note that $\alpha + \beta = \sum_{i=1}^{p-1} \zeta^i = -1$. So, the equation $X^2 + X + \alpha\beta = 0$ has α, β as its roots. As H is a index 2 subgroup of the full Galois group G, $E^H/\boldsymbol{Q}$ is a quadratic extension (according to the Galois correspondence). So, we have $E^H = \boldsymbol{Q}[\alpha] = \boldsymbol{Q}[\beta]$. But it is also equal to $\boldsymbol{Q}[\Delta]$, $\Delta = \sqrt{\delta} = \sqrt{(\alpha - \beta)^2}$.

Here recall the Gauss sum $G_p = \sum \left(\frac{k}{p}\right) e^{2\pi k i/p} = \sum_{s:\text{even}} \zeta^{r^s} - \sum_{t:\text{odd}} \zeta^{r^t} = \alpha - \beta$. We already studied (!) that

$$G_p^2 = \begin{cases} p, & p \equiv 1 \ (\mathrm{mod}\ 4) \\ -p, & p \equiv 3 \ (\mathrm{mod}\ 4) \end{cases},$$

so we have the required conclusion. (By the way $\alpha\beta = \frac{1}{4}((\alpha + \beta)^2 - (\alpha - \beta)^2) = \frac{1}{4}(1 \mp p)$. We did not use it, sorry.)