2017 NAP Lecture Module III, Problem 1, Solutions

May 28,'17, H. Shiga

We wish to recall several fundamental facts among what we have already studied in the previous Modules.

Problem 1-1] Set $f(X) = X^4 + X + 1, P(X) = X^3 - X + 1 \in \boldsymbol{Q}[X]$. Show the procedure to obtain $\gcd(f, P)$ by the Euclidean algorism.

Problem 1-2]. Let α be a solution of the above $f(X) = 0$ and set $E = \boldsymbol{Q}[\alpha]$. Show the inverse of $P(\alpha)$ in E, provided $P(\alpha) \neq 0$.

Problem I-3]. Let F be a field and let $f(X)$ be an irreducible polynomial in $F[X]$. Let α be a root of $f(X)$. By using the Euclidean method, show that any $Q[\alpha] \in F[\alpha] - \{0\}$ has its inverse in $F[\alpha]$.

(This means that $F(\alpha) = F[\alpha]$. So, in this case, we write $F[\alpha]$ instead of the field $F(\alpha)$ in the later sections).

[Solutions]

1-1,2] Set $Q_1 = x, Q_2 = x, Q_3 = -1/2x - 1/4, R_1 = 1 + x^2, R_2 = 1 - 2x, R_3 = 5/4$. By the Eucidean algorism we have $1 = 4/5((1 + Q_2Q_3)f + (-Q_3 - Q_1 - Q_2Q_3Q_1)P)$. Setting $U(X) = \frac{1}{5}(1 - 2x + x^2 + 2x^3), V(X) = 1/5(4 - x - 2x^2)$, we have $U(X)P(X) + V(X)f(X) = 1$. So $P(\alpha)U(\alpha) = 1$ in $\boldsymbol{Q}[\alpha]$. Hence $U(\alpha) = P(\alpha)^{-1}$.

1-3] Because $f(X)$ is irreducible, by the Euclidean algorism we have some $U(X), V(X) \in F[X]$ such that $U(X)Q(X) + V(X)f(X) = 1$. It means $U(\alpha)Q(\alpha) = 1$ in $F[\alpha]$.

1-4) Set $g(X) = X^3 - p = X^3 - 0 \cdot X^2 - 0 \cdot X - p = a_0X^3 + a_1X^2 + a_2X + a_3$. It holds $p \not| a_0, p|a_i (i = 1, 2, 3), p^2 \not| a_3$. By the Eisenstein criterion = Prop. 1.16, $f(X) \in \boldsymbol{Q}[X]$ is irreducible.

1-5) $F = \boldsymbol{Q}[\alpha]$ is contained in $\boldsymbol{R}$. On the other hand, $X^3 - 2$ has complex roots $\alpha' = \omega\alpha, \alpha'' = \omega^2\alpha, (\omega = e^{2\pi i/3})$. So F does not contain the conjugates α', α''. It means that $F/\boldsymbol{Q}$ is not a normal extension. By observing the condition Thm. 1.10 (c), $\boldsymbol{Q}[\alpha]/\boldsymbol{Q}$ is not a Galois extension.

[Irreducibility of $f(X)$] First, we note that $f(X)$ is reducible in $\boldsymbol{Q}[X] \Longleftrightarrow$ reducible in $\boldsymbol{Z}[X]$ (Gauss' lemma = Prop. 1.13).

(i) $f(X)$ does not have a decomposition into quadratic polynomials in $\boldsymbol{Z}[X]$.

Because] If we have $f(X) = (x^2 + a_1X + b_1)(x^2 + a_2X + b_2), (a_1, a_2, b_1, b_2 \in \boldsymbol{Z})$ By its expansion, we obtain $a_2 = -a_1, b_2 = a_1^2 - b_1$. Cosequently, $f(X) = (a_1^2 - b_1)b_1 + a_1((a_1^2 - b_1) - b_1)x + x^4$. So, we must have $|a_1| = |b_1| = 1$. But in this case the constant term can not be 1.

(ii) $f(X)$ has no linear component.

Because] $f(X)$ has no solution as an element of $\boldsymbol{F}_7[X]$, so $f(X)$ has no solution as an element of $\boldsymbol{Z}[X]$.

By the above arguments, we obtain that $f(X)$ is irreducible in $\boldsymbol{Q}[X]$.