MATH 4E03/6E03 Galois Theory, Fall 2014
Homework 5 Solution

Total: 16 marks. No mark for any unjustified arguments using tables or calculators.

(1) Choose a root α of an irreducible quadratic polynomial over $\mathbb{F}_3 = \{0, 1, 2\}$ and write down the cyclic group structure of $\mathbb{F}_9^\times$ (similar to the example $\mathbb{F}_8^\times$ I did in class). (2 marks)

Answer: Choose $X^2 + X + 2$ which is irreducible over $\mathbb{F}_3$ (since it has no root in $\mathbb{F}_3$.) We take a root α and write

$$\mathbb{F}_9^\times = \{1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}.$$

If we take $\zeta = \alpha$, then we have

$$\begin{aligned}
\zeta &= \alpha, \\
\zeta^2 &= \alpha^2 = -\alpha - 2 = 2\alpha + 1, \\
\zeta^3 &= \alpha(2\alpha + 1) = 2(2\alpha + 1) + \alpha = 2\alpha + 2, \\
\zeta^4 &= \alpha(2\alpha + 2) = 2(2\alpha + 1) + 2\alpha = 2, \\
\zeta^5 &= 2\alpha = 2\zeta, \\
\zeta^6 &= 2\zeta^2 = \alpha + 2, \\
\zeta^7 &= 2\zeta^3 = \alpha + 1, \\
\zeta^8 &= 1.
\end{aligned}$$

□

(2) Using the method shown in class (Lemma 2 and 3), show that the discriminant of an irreducible cubic polynomial of the form $X^3 + bX + c$ is equal to $-4b^3 - 27c^2$. (2 marks)

Answer: Using Lemma 2 in class, we have

$$\Delta = \det \begin{bmatrix} \lambda_0 & \lambda_1 & \lambda_2 \\ \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_2 & \lambda_3 & \lambda_4 \end{bmatrix},$$

where $\lambda_i = \alpha_1^i + \alpha_2^i + \alpha_3^i$ the sum of ith powers of roots. To compute λ_i we apply Newton's identities (Lemma 3 in class):

$$\begin{aligned}
& & &\lambda_0 = \text{ number of roots } = 3, \\
& & &\lambda_1 = \text{ sum of roots } = 0, \\
2b + 0\lambda_1 + \lambda_2 &= 0 &\Rightarrow \quad &\lambda_2 = -2b, \\
3c + b\lambda_1 + 0\lambda_2 + \lambda_3 &= 0 &\Rightarrow \quad &\lambda_3 = -3c, \\
c\lambda_1 + b\lambda_2 + 0\lambda_3 + \lambda_4 &= 0 &\Rightarrow \quad &\lambda_4 = 2b^2,
\end{aligned}$$

Therefore

$$\Delta = \det \begin{bmatrix} 3 & 0 & -2b \\ 0 & -2b & -3c \\ -2b & -3c & 2b^2 \end{bmatrix} = -4b^3 - 27b^2.$$

□

(3) Suppose $\mathrm{char}(K) \neq 2$. Let $f = X^4 + pX^2 + qX + r \in K[X]$ be an irreducible and separable quartic polynomial, and L/K be its splitting field extension. Denote by $\Delta = \delta^2$ its discriminant, and assume that $\delta \notin K$. Let $g \in K[X]$ be the resolvent cubic of f, and assume it has one and only one root $t \in K$. In this situation, I showed in class the following fact from Kappe-Warren,

$$\Gamma(L/K) \cong \begin{cases} \mathbb{Z}_4 & \text{if both } X^2+t \text{ and } X^2-(p-t)X+r \text{ split over } K(\delta), \\ D_8 & \text{otherwise.} \end{cases}$$

The question is to refine the above conditions such that they only involve the base field K.

(a) Show that if an element $a \in K$ is not a square but is a square in $K(\delta)$, then $a = b^2\Delta$ for some $b \in K$. (1 mark)

Answer: Let $a = (c + b\delta)^2 = c^2 + 2bc\delta + b^2\Delta \in K$, then we have $2bc = 0$. In $\mathrm{char}(K) \neq 2$, we have $bc = 0$, and so either $b = 0$ or $c = 0$. If $b = 0$, then $a = c^2$, which contradicts the assumption that a is a non-square in K. Hence $c = 0$ and $a = b^2\Delta$. □

(b) Show that for each of the two quadratic polynomials above, its discriminant is either 0 or a non-square in K. (1 mark)

Answer: We only prove the assertion for $\Delta_1 = \mathrm{disc}(X^2 + t)$, while the proof for $\Delta_2 = \mathrm{disc}(X^2 - (p-t)X + r)$ is similar. Suppose that $\Delta_1 \neq 0$, then the polynomial $X^2 + t$ has distinct roots, i.e., $\alpha_1 + \alpha_2 \neq \alpha_3 + \alpha_4$. If Δ_1 is a square in K, then the polynomial $X^2 + t$ is reducible, i.e., $\alpha_1 + \alpha_2 \in K$. Now remember that in the given situation, the Galois group $\Gamma(L/K)$ is isomorphic to either $\mathbb{Z}_4$ or D_8. Take $\sigma = (1\ 3\ 2\ 4) \in \Gamma(L/K)$, then we have

$$\alpha_1 + \alpha_2 = \sigma(\alpha_1 + \alpha_2) = \alpha_3 + \alpha_4,$$

which is a contradiction. Therefore, Δ_1 has to be non-square in K. □

(c) Show that in the above setting, we have

$$\Gamma(L/K) \cong \begin{cases} \mathbb{Z}_4 & \text{if both } -4t\Delta \text{ and } ((p-t)^2-4r)\Delta \text{ are squares in } K, \\ D_8 & \text{otherwise.} \end{cases}$$

(1 mark)

Answer: We have to show that

$$X^2 + t \text{ splits over } K(\delta) \text{ if and only if } -4t\Delta \text{ is a square in } K$$

and

$$X^2 - (p-t)X + r \text{ splits over } K(\delta) \text{ if and only if } ((p-t)^2 - 4r)\Delta \text{ is a square in } K.$$

Again we only prove the first statement, while the proof of the another is similar. We seperate into two cases.

- If $\Delta_1 = -4t = 0$, then $t = 0$ in $\mathrm{char}(K) \neq 2$ and $X^2 + t = X^2$ clearly splits over $K(\delta)$. Also $-4t\Delta = 0$ is clearly a square in K.
- If $\Delta_1 = -4t \neq 0$, then notice that

$$X^2 + t \text{ splits over } K(\delta) \qquad \Leftrightarrow \qquad \Delta_1 = -4t \text{ is a square in } K(\delta).$$

We know from (b) that $-4t$ is a non-square in K, so by using (a) we have

$$\Delta_1 = -4t \text{ is a square in } K(\delta) \qquad \Leftrightarrow \qquad -4t\Delta \text{ is a square in } K.$$

□

(You may need to recall that, because we have set $t = \theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, the realization of $\mathbb{Z}_4$ is

$$\{\mathrm{Id}_L,\ (1\ 3\ 2\ 4),\ (1\ 2)(3\ 4),\ (1\ 4\ 3\ 2)\},$$

and the realization of D_8 is

$$\{\mathrm{Id}_L,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3\ 2\ 4),\ (1\ 4\ 3\ 2),\ (1\ 3)(2\ 4),\ (1\ 4)(3\ 2)\},$$

both as subgroups permuting the roots.)

(4) (Garling Ex 15.3) If p is a prime, show that for every positive integer n,

$$\Phi_{p^n}(X) = 1 + X^{p^{n-1}} + X^{2p^{n-1}} + \cdots + X^{(p-1)p^{n-1}}.$$

(2 marks)

Answer: Recall the definition for $\Phi_N(X)$, that

$$\Phi_N(X) = \frac{X^N - 1}{\prod_{d|N \text{ but } d \neq N} \Phi_d(X)}.$$

When $N = p^n$, the proper divisors of N are 1, p, p^2, $\ldots$, p^{n-1}. Therefore ,we have

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{\prod_{j=0}^{n-1} \Phi_{p^j}(X)}.$$

If we apply induction here, then by induction assumption the denominator is equal to $X^{p^{n-1}} - 1$. Hence

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = \frac{(X^{p^{n-1}})^p - 1}{X^{p^{n-1}} - 1}.$$

If we write $Y = X^{p^{n-1}}$, then he above is equal to

$$\frac{Y^p - 1}{Y - 1} = 1 + Y + Y^2 + \cdots + Y^{p-1} = 1 + X^{p^{n-1}} + X^{2p^{n-1}} + \cdots + X^{(p-1)p^{n-1}}.$$

$\square$

(5) (Garling Ex 15.6) Suppose that p is a prime number which does not divide a positive integer m. Let ζ be a primitive mth root of unity over $\mathbb{Z}_p$.

(a) Show that $[\mathbb{Z}_p(\zeta) : \mathbb{Z}_p]$ is equal to the order of p in the multiplicative group

$$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m \text{ which is invertible}\} = \{a \in \mathbb{Z}_m \text{ where } (a, m) = 1\}.$$

(1 mark)

Answer: Remember that every field extension of $\mathbb{Z}_p$ must be of the form $\mathbb{F}_{p^k}$ for a certain positive integer k, and its multiplicative subgroup contains all $(p^k - 1)$th roots of unity (not necessarily primitive). Since $\mathbb{Z}_p(\zeta)$ is the smallest field extension of $\mathbb{Z}_p$ containing the mth root of unity ζ, the degree $k = [\mathbb{Z}_p(\zeta) : \mathbb{Z}_p]$ must be the smallest k such that ζ is a $(p^k - 1)$root of unity. This implies that

$$p^k - 1 \text{ is a multiple of } m, \qquad \text{(1 mark for this key observation)}$$

or $p^k \equiv 1 \mod m$, with k being the smallest positive integer satisfying this property. In other words, k is the multiplicative order of p mod m. $\square$

(b) Show that

$$\text{the cyclotomic polynomial } \Phi_m \text{ is irreducible over } \mathbb{Z}_p$$

if and only if

$$\mathbb{Z}_m^\times \text{ is a cyclic group generated by } p.$$

(Notice here a group generated by p is the one of the form $\{p, p^2, p^3, \dots\}$.) (2 marks)

Answer: ($\Rightarrow$) Suppose that Φ_m is irreducible, then $[\mathbb{Z}_p(\zeta) : \mathbb{Z}_p] = \deg \Phi_m = \phi(m) = \#\mathbb{Z}_m^\times$. We know that $\mathbb{Z}_p(\zeta)$ is a splitting field of $X^m = 1$, so that $\mathbb{Z}_p(\zeta)/\mathbb{Z}_p$ is a Galois extension and so $\#\Gamma(\mathbb{Z}_p(\zeta)/\mathbb{Z}_p) = [\mathbb{Z}_p(\zeta) : \mathbb{Z}_p] = \#\mathbb{Z}_m^\times$. Recall from Theorem 15.4 that $\Gamma(\mathbb{Z}_p(\zeta)/\mathbb{Z}_p)$ is isomorphic to a subgroup of $\mathbb{Z}_m^\times$. The above equality of orders implies that indeed $\Gamma(\mathbb{Z}_p(\zeta)/\mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_m^\times$. In particular, $\mathbb{Z}_m^\times$ is cyclic, because it is the Galois group of an extension of a finite field. We know it is generated by p from (a).
($\Leftarrow$) Let m_ζ be the minimal polynomial of ζ over $\mathbb{Z}_p$. The aim is to show that $\deg m_\zeta = \deg \Phi_m = \phi(m)$. We know that $\deg m_\zeta = \#\Gamma(\mathbb{Z}_p(\zeta)/\mathbb{Z}_p)$. By (a), the order of the Galois group is the multiplicative order of p in $\mathbb{Z}_m$. By the given condition, this multiplicative order is $\phi(m)$.

□

Remark: Some of you assume that Φ_m is irreducible throughout the solution, which is not true. Remember that Φ_m is irreducible in $\mathbb{Q}[X]$, but is not necessarily irreducible in $\mathbb{Z}_p[X]$.

(6) Let p be an odd prime number, and denote the primitive pth root of unity $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$. Define the following sum (an example of *Gauss sum*)

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a,$$

where $\left(\frac{a}{p}\right)$ is the *Legendre symbol* (not the rational number $\frac{a}{p} \in \mathbb{Q}$), defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{otherwise.} \end{cases}$$

Hence $a \mapsto \left(\frac{a}{p}\right)$ is indeed a function on $\mathbb{Z}_p^\times$; in other words, we have $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.

(a) Show that $G^2 = \left(\frac{-1}{p}\right) p$ (again $\left(\frac{-1}{p}\right)$ is the Legendre symbol). (2 marks) (Hint: You may use the fact that half of the elements in $\mathbb{Z}_p^\times$ are squares, and another half are not.)

Answer: We compute directly that

$$G^2 = \left(\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a\right) \left(\sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta_p^b\right).$$

Since $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, we have

$$G^2 = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta_p^{a+b}.$$

We then change variable by writing $b = ac$ for $c = 1 \cdots, p-1$, and rewrite the above sum as

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

We separate the sum by the conditions $c = p-1$ and $c \neq p-1$. When $c = p-1$, the sum is equal to

$$\sum_{a=1}^{p-1} \left(\frac{-1}{p}\right) \zeta_p^{a(1-1)} = \sum_{a=1}^{p-1} \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)(p-1).$$

For each $c \neq p-1$, the sum is equal to

$$\sum_{a=1}^{p-1} \left(\frac{c}{p}\right) \zeta_p^{a(1+c)} = \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{a(1+c)}. \tag{1}$$

Notice that the set $\{\zeta_p^{a(1+c)}$, where $a = 1, \cdots, p-1\}$ contains exactly all the pth roots of unity except 1, so the sum is equal to -1. Therefore, the equation (1) above is equal to $-\left(\frac{c}{p}\right)$. Finally we sum up all the terms with $c = 1, \ldots, p-2, p-1$ and obtain

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

The first sum $-\sum_{c=1}^{p-2} \left(\frac{c}{p}\right)$ is equal to $\left(\frac{-1}{p}\right)$, since the given hint implies that $\sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = 0$. Therefore,

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

$\square$

(b) Prove the following particular example of *Kronecker-Weber Theorem*: Every quadratic extension is contained in a cyclotomic extension over $\mathbb{Q}$. (2 marks)

Answer: Remember that every quadratic extension is of the form $\mathbb{Q}(\sqrt{N})$ for some integer $\sqrt{N}$. We can assume N is positive since we know that $\mathbb{Q}(\sqrt{-1})$ is cyclotomic. Therefore, it is enough to show that for each prime number p, we have $\sqrt{p} \in \mathbb{Q}(\zeta_m)$ for some sufficiently large integer m. If $p = 2$, then we know that $\sqrt{2} \subseteq \mathbb{Q}(\zeta_8)$ because $\zeta_8 = \frac{1+\sqrt{-1}}{\sqrt{2}}$. If p is odd, then recall from (a) that $G^2 = \left(\frac{-1}{p}\right) p$, we have $\sqrt{p} = \sqrt{\left(\frac{-1}{p}\right)} G$. We know that $\sqrt{\left(\frac{-1}{p}\right)} \in \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ and $G \in \mathbb{Q}(\zeta_p)$, so $\sqrt{p} = \sqrt{\left(\frac{-1}{p}\right)} G \in \mathbb{Q}(\zeta_{4p})$. $\square$

Remark: Some of you mistakenly wrote $\sqrt{p} = G \in \mathbb{Q}(\zeta_p)$, which is not true in the case when $\left(\frac{-1}{p}\right) = -1$. Some of you forgot to consider $\mathbb{Q}(\sqrt{\pm 2}) \subseteq \mathbb{Q}(\zeta_8)$.

Remark: The full form of Kronecker-Weber Theorem asserts that if $L/\mathbb{Q}$ is a Galois extension such that $\Gamma(L/\mathbb{Q})$ is an abelian group, then L is contained in a cyclotomic extension over $\mathbb{Q}$. We can even find the smallest such cyclotomic extension. The theorem is highly non-trivial in algebraic number theory, and has many important consequences. For example, the above example of Kronecker-Weber Theorem implies the quadratic reciprocity:

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

for all distinct odd prime numbers p and q.