Graduate Algebra
Homework 10

Due 2015-04-22

1. (a) Let p be a prime and $n \geq 1$. Show that there exists a subextension $\mathbb{Q}(\zeta_{p^{n+2}})/K/\mathbb{Q}$ with $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$.

   (b) Let G be any finite abelian group. Show there exists a Galois extension $K/\mathbb{Q}$ with $\text{Gal}(K/\mathbb{Q}) \cong G$.

Proof. (1): Note that $\text{Gal}(\mathbb{Q}(\zeta_{p^{n+2}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+2}\mathbb{Z})^\times$ which always has as a subquotient $\mathbb{Z}/p^n\mathbb{Z}$. Indeed, if $p > 2$ then $(\mathbb{Z}/p^{n+2}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{n+1}\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. If $p = 2$ then $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$.

Let G be the kernel of this surjection in which case $\text{Gal}(\mathbb{Q}(\zeta_{p^{n+2}})^G/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ from Galois theory.

(2): If G is finite abelian write $G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$. Let $K_i \subset \mathbb{Q}(\zeta_{p_i^{n_i+2}})$ be the subfield from above such that $\text{Gal}(K_i/\mathbb{Q}) \cong \mathbb{Z}/p_i^{n_1}\mathbb{Z}$. Then $K_i \cap K_j = \mathbb{Q}$ because $[K_i \cap K_j : \mathbb{Q}] \mid ([K_i : \mathbb{Q}], [K_j : \mathbb{Q}]) = (p_i^{n_i}, p_j^{n_j}) = 1$. Then $K_1 \cdots K_k$ is Galois over $\mathbb{Q}$ with Galois group $\text{Gal}(\prod K_i/\mathbb{Q}) \cong \prod \text{Gal}(K_i/\mathbb{Q}) \cong \prod \mathbb{Z}/p_i^{n_1}\mathbb{Z} \cong G$ as desired. □

2. (a) Show that the discriminant of the polynomial $X^n + pX + q$ is

$$(-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

   (b) If $p > 2$ is a prime show that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subset \mathbb{Q}(\zeta_p)$. [Hint: Compute the discriminant of $X^p - 1$.]

Proof. (1): From class $D = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$. But $f'(\alpha_i) = n\alpha_i^{n-1} + p$ and $\alpha_i^{n-1} = -p - q\alpha_i^{-1}$ so $f'(\alpha_i) = n(-p - q/\alpha_i) + p = (n-1)p/\alpha_i(-\alpha_i - qn/((n-1)p))$.

Thus

$$\begin{aligned}
D &= (-1)^{\binom{n}{2}} \prod f'(\alpha_i) \\
&= (-1)^{\binom{n}{2}} \prod \frac{(n-1)p}{\alpha_i} \left(-\alpha_i - \frac{qn}{p(n-1)}\right) \\
&= (-1)^{\binom{n}{2}} \frac{((n-1)p)^n}{\prod \alpha_i} f\left(-\frac{qn}{p(n-1)}\right) \\
&= (-1)^{\binom{n}{2}} \frac{(n-1)^n p^n}{(-1)^n q} \left(\left(-\frac{qn}{p(n-1)}\right)^n + p\left(-\frac{qn}{p(n-1)}\right) + q\right) \\
&= (-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n
\end{aligned}$$

since $\prod \alpha_i = (-1)^n q$.

(2): The discriminant of $X^p - 1$, using (1), is $D = (-1)^{\binom{p}{2}} p^p (-1)^{p-1} = (-1)^{(p-1)/2} p^p$ as $\binom{p}{2} + p - 1$ and $(p-1)/2$ have the same parity. But $\sqrt{D} = \prod_{i<j}(\alpha_i - \alpha_j) \in \mathbb{Q}(\zeta_p)$ and so $\sqrt{D} = p^{(p-1)/2}\sqrt{(-1)^{(p-1)/2}p} \in \mathbb{Q}(\zeta_p)$ and so $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subset \mathbb{Q}(\zeta_p)$. □

3. (a) Let $P(X) \in \mathbb{Q}[X]$ be irreducible with prime degree q and exactly two nonreal roots. Show that P has Galois group S_q. [Hint: S_q is generated by a transposition and a q-cycle.]

   (b) Compute the Galois group of $X^7+X+13 \in \mathbb{Q}[X]$. [Hint: You are welcome to use Wolfram Alpha for factorizations.]

Proof. (1): Let $\{\alpha_1, \ldots, \alpha_q\}$ be the set of roots and let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_q)$ be the splitting field. Complex conjugation in $\mathbb{C}$ restricts to a nontrivial automorphism of K as it flips two of the roots. As a permutation of the sets of roots of P complex conjugation is the transposition of the two nonreal complex conjugate roots. The Galois group G had order divisible by q as $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = q \mid [K : \mathbb{Q}]$. Thus there exists an element $g \in G$ of order exactly q. As a permutation of the roots it has to be a q-cycle. Finally, a transposition and a q-cycle generate S_q and so $G \cong S_q$.

(2): The polynomial $P(X) = X^7 + X + 13$ is irreducible. Mod 2 it is irreducible so the Galois group has a 7-cycle. The mod 59 factorization has one cubic and four linears so the Galois group has a 3-cycle. Thus the Galois group contains A_7 which is generated by a 3-cycle and a 7-cycle. Finally, the discriminant is not a square so the Galois group is S_7.

□

4. Let $L/K/\mathbb{Q}$ be finite extensions and denote by R and S the integral closure of $\mathbb{Z}$ in K and L respectively.

   (a) Show that $\operatorname{Tr}_{L/K} : L \to K$ restricts to $\operatorname{Tr}_{L/K} : S \to R$.

   (b) Show that $\mathcal{ID} = \{x \in L | \operatorname{Tr}_{L/K}(xS) \subset R\}$ is an S-submodle of L and that $\mathcal{D} = \{x \in S | x\mathcal{ID} \subset S\}$ is an ideal of S.

   (c) Suppose $K = \mathbb{Q}$ and so $R = \mathbb{Z}$. Also suppose that $L = \mathbb{Q}(\alpha)$ and $S = \mathbb{Z}[\alpha]$ and let $m_\alpha(X) \in \mathbb{Z}[X]$ be its minimal polynomial over $\mathbb{Z}$, of degree d.

      i. Show that $\dfrac{1}{m_\alpha(X)} \in X^{-d}(1 + X^{-1}\mathbb{Z}[\![X^{-1}]\!])$.

      ii. Show that $\dfrac{1}{m_\alpha(X)} = \sum_{i=1}^{d} \dfrac{1}{m'_\alpha(\alpha_i)(X - \alpha_i)}$ where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ are the roots of $m_\alpha(X)$.
      Conclude that $\dfrac{1}{m_\alpha(X)} = \sum_{n \geq 1} X^{-n} \operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}} \left(\dfrac{\alpha^{n-1}}{m'_\alpha(\alpha)} \right)$.

      iii. Show that
$$\operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}} \left(\frac{\alpha^n}{m'_\alpha(\alpha)} \right) = \begin{cases} 0 & 0 \leq n < d-1 \\ 1 & n = d-1 \\ \in \mathbb{Z} & n \geq d \end{cases}$$

      iv. Deduce that $m'_\alpha(\alpha) \in \mathcal{D}$. (One can actually show that $\mathcal{D}$ is generated by $m'_\alpha(\alpha)$.) [Hint: Use (iii).]

Proof. (a): Suppose $\alpha \in S$, i.e., it is integral over $\mathbb{Z}$. Thus the minimal polynomial of α over $\mathbb{Q}$ is monic in $\mathbb{Z}[X]$. Any automorphism $\sigma \in \operatorname{Gal}(L/K)$ takes α to another root of its minimal polynomial and so $\sigma(\alpha)$ is again integral over $\mathbb{Z}$. Finally, $\operatorname{Tr}_{L/K}(\alpha)$ is a sum of elements of the form $\sigma(\alpha)$ and thus is integral over $\mathbb{Z}$. At the same time it is in K and therefore it is in the integral closure R of $\mathbb{Z}$ in K.

(b): If $\operatorname{Tr}_{L/K}(xS) \subset R$ and $\operatorname{Tr}_{L/K}(yS) \subset R$ and $a \in S$ then $\operatorname{Tr}_{L/K}((x + ay)S) = \operatorname{Tr}_{L/K}(xS) + \operatorname{Tr}_{L/K}(yaS) \subset \operatorname{Tr}_{L/K}(xS) + \operatorname{Tr}_{L/K}(yS) \subset R$ and so $\mathcal{ID}$ is an S-submodule of L. Suppose now that $x, y \in \mathcal{D}$ and $s \in S$. Then $(x + ay)\mathcal{ID} = x\mathcal{ID} + ya\mathcal{ID} \subset x\mathcal{ID} + y\mathcal{ID} \subset S$ as $a \in S$ and $\mathcal{ID}$ is an S-module. Therefore $\mathcal{D} \subset S$ is an ideal.

(c):

(i): Write $m_\alpha(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Then
$$\frac{1}{m_\alpha(X)} = \frac{X^{-d}}{1 + a_{d-1}X^{-1} + \cdots + a_0 X^{-d}} \in X^{-d}(1 + X^{-1}\mathbb{Z}[\![X^{-1}]\!])$$

as $1 + a_{d-1}X^{-1} + \cdots + a_0 X^{-d} \in \mathbb{Z}[\![X^{-1}]\!]^\times$ with inverse in $1 + X^{-1}\mathbb{Z}[\![X^{-1}]\!]$.

(ii): Write $m_\alpha(X) = \prod(X - \alpha_i)$ in $\mathbb{C}$, separable as the minimal polynomial is irreducible. Then

$$\sum \frac{m_\alpha(X)}{m'_\alpha(\alpha_i)(X - \alpha_i)}$$

is a polynomial that is equal to 1 when evaluated at $X \in \{\alpha_1, \ldots, \alpha_d\}$ (L'Hôpital). But the degree of this polynomial is $d - 1$ and therefore the polynomial is identically 1. Note that the image of α_1 via the embeddings of $\mathbb{Q}(\alpha) \hookrightarrow L$ are the roots $\alpha_1, \ldots, \alpha_d$. Therefore

$$\begin{aligned}
\frac{1}{m_\alpha(X)} &= \sum_i \frac{1}{m'_\alpha(\alpha_i)X(1 - \alpha_i X^{-1})} \\
&= \sum_i \sum_{n \geq 0} \frac{(\alpha_i X^{-1})^n}{m'_\alpha(\alpha_i)X} \\
&= \sum_{n \geq 1} X^{-n} \sum_i \frac{\alpha_i^{n-1}}{m'_\alpha(\alpha_i)} \\
&= \sum_{n \geq 1} X^{-n} \operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}} \left(\frac{\alpha^{n-1}}{m'_\alpha(\alpha)} \right)
\end{aligned}$$

(iii): From (i) and (ii) comparing the coefficient of X^{-n} we deduce the result immediately.

(iv): Throughout $\operatorname{Tr} = \operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$. We need to show that if $x \in \mathcal{ID}$ then $m'_\alpha(\alpha)x \in S = \mathbb{Z}[\alpha]$. Suppose $x \in \mathcal{ID}$ which implies that $\operatorname{Tr}(x\mathbb{Z}[\alpha]) \subset \mathbb{Z}$. This is equivalent to $\operatorname{Tr}(x\alpha^n) \in \mathbb{Z}$ for $0 \leq n \leq d - 1$. Write

$$m'_\alpha(\alpha)x = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \in \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$$

The condition $\operatorname{Tr}(x\alpha^n) \in \mathbb{Z}$ is the same as $\operatorname{Tr}((\sum a_i\alpha^i)\alpha^n / m'_\alpha(\alpha)) \in \mathbb{Z}$ which, using that Tr is linear, yields

$$\sum_{i=0}^{d-1} a_i \operatorname{Tr}(\frac{\alpha^{i+n}}{m'_\alpha(\alpha)}) \in \mathbb{Z}$$

Now show by induction that $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$ which is what we want. Taking $n = 0$ and using (iii) the above trace is simply $a_{d-1} \in \mathbb{Z}$. Suppose $a_{d-1}, \ldots, a_{k+1} \in \mathbb{Z}$. Take $n = d - 1 - k$ so

$$\sum_i a_i \operatorname{Tr}(\alpha^{i+d-1-k}/m'_\alpha(\alpha)) = a_k + \sum_{i=k+1}^{d-1} a_i \operatorname{Tr}(\alpha^{i+d-1-k}/m'_\alpha(\alpha)) \in \mathbb{Z}$$

again using (iii). But in the second sum every factor is in $\mathbb{Z}$ and so $a_k \in \mathbb{Z}$ yielding the inductive step.

□