University of New South Wales

School of Mathematics and Statistics

Assignment 1

Galois Theory

Author:
Edward McDonald

Student Number:
3375335

For this assignment, $n > 1$ and k is a field containing a primitive nth root of unity ζ_n, and the characteristic of k does not divide n. Let $a \in k$ be such that the polynomial $P_a(x) = x^n - a$ has no root in k. Let $K_{a,n} = k(\sqrt[n]{a})$ be a field extention of k generated by a root of P_a.

Question 1

Lemma 1. *In $K_{a,n}$, P_a is expressed as a product of n distinct linear factors*

$$P_a(x) = \prod_{k=1}^{n} (x - \zeta_n^k \sqrt[n]{a})$$

Proof. Since ζ_n is primitive, all of the elements $\zeta_n^k \sqrt[n]{a}$ for $k = 1, 2, \ldots, n$ are distinct and are all zeroes of P_a. Hence since P_a has at most n roots, this is all of the roots of P_a and so P_a decomposes as

$$P_a(x) = \prod_{k=1}^{n} (x - \zeta_n^k \sqrt[n]{a})$$

□

Question 2

For this question, $\lambda \in \mathbb{Z}/n$ and define

$$\sigma_\lambda : K_{a,n} \to K_{a,n}$$

by $\sigma_\lambda(f(\sqrt[n]{a})) = f(\zeta_n^\lambda \sqrt[n]{a})$ for any polynomial $f \in k[x]$.

Theorem 1. *σ_λ is a field automorphism on $K_{a,n}$.*

Proof. First since any $x \in K_{a,n}$ can be written uniquely as a sum

$$x = b_0 + b_1 \sqrt[n]{a} + b_2 \sqrt[n]{a^2} + \cdots + b_{n-1} \sqrt[n]{a^{n-1}}, \tag{1}$$

for $b_i \in k$, then $\sigma_\lambda(x)$ is given by

$$\sigma_\lambda(x) = b_0 + b_1 \sqrt[n]{a}\zeta_n^\lambda + b_2 \sqrt[n]{a^2}\zeta_n^{2\lambda} + \cdots + b_{n-1} \sqrt[n]{a^{n-1}}\zeta_n^{\lambda(n-1)}. \tag{2}$$

This shows that σ_λ is well defined, since the expression in equation 1 is unique so σ_λ must be given by 2.
To show that σ_λ is bijective, it suffices to find an inverse function. Let $x = f(\sqrt[n]{a}) \in K_{a,n}$, then

$$\sigma_\lambda(\sigma_{-\lambda}(x)) = f(\sqrt[n]{a}\zeta_n^\lambda \zeta_n^{-\lambda}) = x = \sigma_{-\lambda}(\sigma_\lambda(x)).$$

Suppose that $f(\sqrt[n]{a}), g(\sqrt[n]{a}) \in K_{a,n}$. Then,

$$\begin{aligned}
\sigma_\lambda(f(\sqrt[n]{a}) + g(\sqrt[n]{a}) &= \sigma_\lambda((f+g)(\sqrt[n]{a})) \\
&= (f+g)(\sqrt[n]{a}\zeta_n^\lambda) \\
&= f(\sqrt[n]{a}\zeta_n^\lambda) + g(\sqrt[n]{a}\zeta_n^\lambda) \\
&= \sigma_\lambda(f(\sqrt[n]{a})) + \sigma_\lambda(g(\sqrt[n]{a})).
\end{aligned}$$

Hence the function σ_λ is additive. An identical argument shows that σ_λ is multiplicative.

□

Corollary 1. *For $\lambda \in \mathbb{Z}/n$, $\sigma_\lambda \in \mathrm{Aut}(K_{a,n}/k)$.*

Proof. Let $b \in k$, then we have $\sigma_\lambda(b) = b$ since b is a degree 0 polynomial in $k[x]$.
Hence σ_λ fixes k. □

Question 3

Lemma 2. *If $\sigma \in \mathrm{Aut}(K_{a,n}/k)$, then $P_a(\sigma(\sqrt[n]{a})) = 0$.*

Proof. We simply compute $P_a(\sigma(\sqrt[n]{a}))$,

$$\begin{aligned}
P(\sigma(\sqrt[n]{a})) &= \sigma(\sqrt[n]{a})^n - a \\
&= \sigma(\sqrt[n]{a}^n) - a \\
&= \sigma(a) - \sigma(a) \\
&= 0.
\end{aligned}$$

□

Lemma 3. *If $\sigma \in \mathrm{Aut}(K_{a,n}/k)$, then $\sigma = \sigma_\lambda$ for some $\lambda \in \mathbb{Z}/n$.*

Proof. We have shown that $\sigma(\sqrt[n]{a})$ is a root of P_a, however the only roots of P_a over $K_{a,n}$ are of the form $\zeta_n^\lambda \sqrt[n]{a}$ for some $\lambda \in \mathbb{Z}/n$. Hence $\sigma(\sqrt[n]{a}) = \zeta_n^\lambda \sqrt[n]{a}$. Since $\{1, \sqrt[n]{a}\}$ generates $K_{a,n}$ as a k-space, this uniquely determines σ as σ_λ. □

Theorem 2. *Hence, $\mathrm{Aut}(K_{a,n}/k)$ is isomorphic to $\mathbb{Z}/n$ as a group.*

Proof. The map $\lambda \mapsto \sigma_\lambda$ is a bijection since we have shown that it is surjective, and if $\sigma_\lambda = \sigma_\mu$, then $\zeta_n^\lambda = \zeta_n^\mu$ so $\lambda = \mu$ as ζ_n is primitive. To show that this is a group homomorphism, let $\lambda, \mu \in \mathbb{Z}/n$. Then $\sigma_\lambda \circ \sigma_\mu$ is a field automorphism fixing k, and $\sigma_\lambda(\sigma_\mu(\sqrt[n]{a})) = \sqrt[n]{a}\zeta_n^\mu\zeta_n^\lambda = \sqrt[n]{a}\zeta_n^{\lambda+\mu}$. Hence $\sigma_\lambda \circ \sigma_\mu = \sigma_{\lambda+\mu}$. Hence we have an isomorphism of groups. □

Question 4

For this question, $m|n$ is an integer, and $m(\mathbb{Z}/n)$ is the subgroup of $\mathbb{Z}/n$ generated by m.

Lemma 4. *$\sqrt[m]{a}$ is fixed by σ_λ for each $\lambda \in m(\mathbb{Z}/n)$.*

Proof. Note that $\sqrt[m]{a} = \sqrt[n]{a}^{n/m}$ since n/m is an integer. Hence $\sigma_\lambda(\sqrt[m]{a}) = \sqrt[n]{a}^{n/m}\zeta_n^{n\lambda/m} = \sqrt[n]{a}\zeta_n^{n\lambda/m}$ Hence σ_λ fixes $\sqrt[n]{a}$ if and only if $n|n\lambda/m$, so we must have $m|\lambda$. Hence $\lambda \in m(\mathbb{Z}/n)$. □

Theorem 3. *$\sigma_\lambda(u) = u$ for all $\lambda \in m(\mathbb{Z}/n)$ if and only if $u \in K_{a,m}$.*

Proof. Suppose first that $u \in K_{a,m}$. It is sufficient to consider the case $u = \sqrt[m]{a}$ since $\sqrt[m]{a}$ generates $K_{a,m}$ as a k-algebra. We have already shown for this case that $\sigma_\lambda(u) = u$ for all $\lambda \in m(\mathbb{Z}/n)$. Conversely, assume that $\sigma_\lambda(u) = u$ for each $\lambda \in m(\mathbb{Z}/n)$. We know that u can be uniquely written as

$$u = b_0 + b_1\sqrt[n]{a} + \cdots + b_{n-1}\sqrt[n]{a}^{n-1}.$$

for $b_i \in k$. Then if $\sigma_\lambda(u) = u$, we have

$$b_0 + b_1\sqrt[n]{a}\zeta_n^\lambda + \cdots + b_{n-1}\sqrt[n]{a}^{n-1}\zeta_n^{\lambda(n-1)} = b_0 + b_1\sqrt[n]{a} + \cdots + b_{n-1}\sqrt[n]{a}^{n-1}.$$

Hence by the uniqueness of this representation, we have $b_i = \zeta_n^{\lambda i} b_i$ for all $i = 0, \ldots, n-1$, and for all $\lambda \in m(\mathbb{Z}/n)$. If $b_i \neq 0$, we must have $\zeta_n^{\lambda i} = 1$, in particular $\zeta_n^{mi} = 1$. So $n|mi$. Hence there is some integer p such that $pn/m = i$. Thus, we can only have $b_i \neq 0$ when i is a multiple of n/m. Hence each term in the expression of u is a multiple of a power of $\sqrt[n]{a}^{n/m} = \sqrt[m]{a}$.
Thus, $u \in K_{a,m}$.
If $u \in K_{a,m}$, we must prove that $\sigma_\lambda(u) = u$ for all $\lambda \in m(\mathbb{Z}/n)$. However it is sufficent to consider $u = \sqrt[m]{a} = \sqrt[n]{a}^{n/m}$ since this generates $K_{a,m}$ as a k-algebra. Clearly then $\sigma_\lambda(u) = \sqrt[m]{a}\zeta_n^{n\lambda/m}$. However since λ is a multiple of m, we conclude that $\zeta_n^{n\lambda/m} = 1$. □