MATH5725: Galois Theory (2014, S2) Assignment 2

Due Date
This assignment is due at 5pm on Wednesday 22 October.

Marks
The assignment is worth 20% of your total mark. It is marked out of 20.

Submission guidelines
You can submit the assignment by email to s.meagher@unsw.edu.au, or by giving me a hard copy, or by uploading to moodle.

Typed submissions are preferred, but if you do not have access to mathematical typesetting software (e.g. latex), or if you are not familiar with the use of such software, handwritten submissions are also acceptable.

Notes on references
If you use a theorem or a formula, you do not need to give a full reference if it is something mentioned in the lectures, but just a short reference will suffice.

Question
Let p be a positive prime number; throughout k will be a field of characteristic p. Therefore the field $\mathbf{F}_p$, with p elements, is a subfield of k.

Recall a Galois Extension K/k is called cyclic if the Galois group $\mathrm{Gal}(K/k)$ is cyclic.

The goal of this question is to classify cyclic Galois extensions K/k such that $[K : k] = p$. The conclusions of Parts 1 and 3 are what is usually referred to as Artin-Schreier theory. This situation is different from characteristic 0 as the degree p cyclic extensions are not obtained by extracting pth roots (and can not be because $X^p - a$ is not a separable polynomial in characteristic p).

Note: in this question the fact that the additive group $\mathbf{Z}/p$ is naturally isomorphic to the additive group of the field with p elements $\mathbf{F}_p$ may be used without comment.

Part 1: The equation $X^p - X - a = 0$
Let $a \in k$ and let $f = X^p - X - a \in k[X]$. Assume that k does not contain a solution to the equation $f(X) = 0$.
(a) Show that f is a separable polynomial. (Hint: see Lecture 4).
(b) Let K/k be the splitting field of f and let $\alpha \in K$ be a solution of $f(X) = 0$. Show that $\alpha + i$ is also a solution of $f(X) = 0$ if $i \in \mathbf{F}_p$ (Hint: if $i \in \mathbf{F}_p$ then $i^p = i$).
(c) Let $2 \leq d \leq p-1$. Show that if there is a degree d polynomial $g \in k[X]$ such that $f = gh$ for some $h \in k[X]$ then $\alpha \in k$. (Hint: find a formula for the coefficient of X^{d-1} of g).
(d) From (c) conclude that f is irreducible. Show that if α is a root of $f(X)$ then $K = k(\alpha)$.
(e) Let $\sigma \in \mathrm{Gal}(K/k)$. Show that σ is determined by the value of $\sigma(\alpha)$ and that $\sigma(\alpha)$ determines a unique element i_σ of $\mathbf{Z}/p$. Show that the map

$$\psi : \mathrm{Gal}(K/k) \longrightarrow \mathbf{Z}/p : \sigma \mapsto i_\sigma$$

is an isomorphism of groups.

Part 2: Traces
Let L/E be a Galois Extension where E is a field of any characteristic. Let $G = \mathrm{Gal}(L/E)$ be its Galois group. The trace $\mathrm{Tr}_{L/E}(\alpha)$ of an element $\alpha \in L$ is defined by the formula

$$\mathrm{Tr}_{L/E}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

(a) Let $G = \{\sigma_1, \cdots, \sigma_n\}$ where $n = |G| = [L : E]$. The functions $\sigma_i|_{L^*}$ will be considered as group homomorphisms from L^* to L^*. Let $\iota : L^* \longrightarrow L$ be the inclusion. A function

$\tau : L^* \longrightarrow L^*$ therefore naturally defines a function $\iota \circ \tau : L^* \longrightarrow L$.[1]

Show that if $\mathrm{Tr}_{L/E}$ is equal to the zero function then the functions $\iota \circ \sigma_i$ are linearly dependent when considered in the L vector space of functions $\mathrm{Hom}(L^*, L)$. Quote a theorem from Lecture 9 that implies that $\mathrm{Tr}_{L/E}$ can therefore not be identically zero.

(b) Now assume that G is cyclic and $\sigma \in G$ is a generator so that

$$G = \{1, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}.$$

Let $\theta \in L$ be an element such that $\mathrm{Tr}_{L/E}(\theta) \neq 0$ (which exists by (a)). Assume given $\beta \in L$ such that $\mathrm{Tr}_{L/E}(\beta) = 0$. Let α be given by the formula

$$\alpha = \frac{1}{\mathrm{Tr}_{L/E}(\theta)}(\beta\sigma(\theta) + (\beta + \sigma(\beta))\sigma^2(\theta) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\theta)).$$

Show that $\beta = \alpha - \sigma(\alpha)$. (Hint: you will need to use the fact that the trace of β is zero).

Part 3: Cyclic Extensions of degree p

Let K/k be Galois with Galois group $\mathrm{Gal}(K/k) = \mathbf{Z}/p$. Let σ be a generator of $\mathrm{Gal}(K/k)$.
(a) Show that $\mathrm{Tr}_{K/k}(1) = 0$ (Hint: k is a field of characteristic p).
(b) Using Part 2(b) show that there is an element $\alpha \in K$ such that $1 = \alpha - \sigma(\alpha)$. Conclude that $\alpha \notin k$ (Hint: k is the fixed field of $\mathrm{Gal}(K/k)$).
(c) Show that $a = \alpha^p - \alpha \in k$. (Hint: first show that the map $K \to K : x \mapsto x^p$ is a field homomorphism).[2]
(d) Show that for each integer i that $\sigma^i(\alpha)$ is a solution of $f(X) = X^p - X - a = 0$.
(e) From (d) and Part 1, show that $k(\alpha)$ is the splitting field of f and that f is irreducible.
(f) By considering degrees, show that $K = k(\alpha)$.

Summary[3]

Parts 1 and 3 imply the following:
K/k is a Cyclic Galois extension of degree p if and only if there exists $a \in k$ such that K is the splitting field of $f = X^p - X - a \in k[X]$. In this case:
(1) f is irreducible;
(2) $K = k(\alpha)$ where α is a root of f; and
(3) $i \in \mathrm{Gal}(K/k) = \mathbf{Z}/p$ acts by $\alpha \mapsto \alpha + i$.

Note: Cyclic Extensions in characteristic p for higher powers of p are handled using the so-called Witt vectors.

[1]Note that if τ is a group homomorphism, that $\iota \circ \tau$ is not because L is not a group under the multiplication. This is the reason for the slightly heavy notation.
[2]Note that it is only a field automorphism if K is perfect.
[3]What follows is not part of the question.