# 1 Introduction to Galois theory assignmens 2, Problem 1

# 2 Introduction to Galois theory assignmens 2, Problem 2

Let $k$ be a field of characteristic $p > 0$, $0 \neq a \in k$, $P = X^p - aX - b \in k[X]$, $K$ splitting field of $P$.

**Problem 2.1** *Why is $K$ a Galois extension of $k$? Show that $X^{p-1} - a$ is split over $K$ and its roots together with 0 form a subgroup of $K$, isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Solution: Obviously by differential it's separable, hence must be galois.

Let $x$ be a root of $P$ and $y$ be a root $X^{p-1} - a$, then by Frobenious mapping:

$$(x+y)^p - a(x+y) - b = P(x) - y(y^{p-1} - a) = y(y^{p-1} - a) = 0$$

So $x + y_i$ where $y_i$ are all roots of $X^{p-1} - a$ are roots of $P$, because $P$ split, hence $X^{p-1} - a$ must split.(Because $x + y_i \in K$ and $x \in K$)

Because any $y_i$ or 0 induce the following mapping:

$$y_i : x \mapsto x + y_i$$

which is an element of $Gal(K/k)$, it forms a group, and of order $p$, which is prime, must be cyclic. □

**Problem 2.2** *What do we know about the Galois group of the splitting field $L$ of the polynomial $X^{p-1} - a$ over $k$?*

Solution: It's subfield of $K$. □

**Problem 2.3** *Let $G = Gal(K/k)$, $H = Gal(K/L)$. Show that for any $g \in G$ and $x$ a root of $P$, $gx - x$ is either zero or a root of $X^{p-1} - a$; moreover for $g \in H$ this element does not depend on $x$.*

Solution:

$$\begin{aligned}
0 &= g(x^p - ax - b) - (x^p - ax - b) = g(x)^p - ag(x) - b - x^p + ax + b \\
&= g(x)^p - x^p - a(g(x) - x) = (gx - x)^p - a(gx - x) \\
&= (gx - x)((gx - x)^{p-1} - a)
\end{aligned}$$

hence $gx - x = 0$ or $gx - x$ is a root of $X^{p-1} - a$.

All roots of $P$ can be written as $x + y_i$, hence $g(x + y_i) - (x + y_i) = gx - x$ for $g \in Gal(K/L)$, hence independent on $x$.

□

**Problem 2.4** *Show that $H$ has either 1 or $p$ elements.*

Solution: From 2.3, we have map

$$h \mapsto hx - x$$

whose images are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Hence must to either trivial or full. $\square$

**Problem 2.5** *Prove the equivalence of the following three properties:*

1. $H = \mathbb{Z}/p\mathbb{Z}$
2. *$P$ is irreducible over $L$*
3. *$P$ is irreducible over $k$*

Solution: $1 \to 2$, $P$ is splitting, have to be irreducible, or the degree less than $p$.

$2 \to 3$, by 2.1, all $Gal(K/k)$ have already $p$ elements, $P$ have to be irreducible.

$3 \to 1$, by 2.4, if not, then $K = L$, impossible for $P$ to be irreducible because $[L : k] \leq p - 1$. $\square$

**Problem 2.6** *Let $k = \mathbb{F}_p(T)$ (the field of rational functions in one variable and coefficients in $\mathbb{F}_p$). What is the order of the Galois group of $P(X) = X^p - TX - T$?*

Solution: Let $L = k(\sqrt[p-1]{T})$, and $P$ is irreducible over $\mathbb{F}_p[T]$, hence $[K : L] = p$. Hence the order is $p(p-1)$.

$\square$