MATH 702 – SPRING 2024
HOMEWORK 5

16. Let $K = \boldsymbol{k}(t)$ be the field of rational functions in one variable over the field $\boldsymbol{k}$. Let G be the subgroup of $\operatorname{Aut}_{\boldsymbol{k}} K$, which is generated by σ and τ where $\sigma(t) = \frac{1}{t}$ and $\tau(t) = 1 - \frac{1}{t}$. Find an element $g \in K$ with $K^G = \boldsymbol{k}(g)$. Prove your answer.

It is easy to check that the elements σ and $\sigma\tau \neq \tau\sigma$ of G have order 2, τ has order 3, and G consists of exactly six elements. (For each of these assertions we need only see what the function in question does to t.)

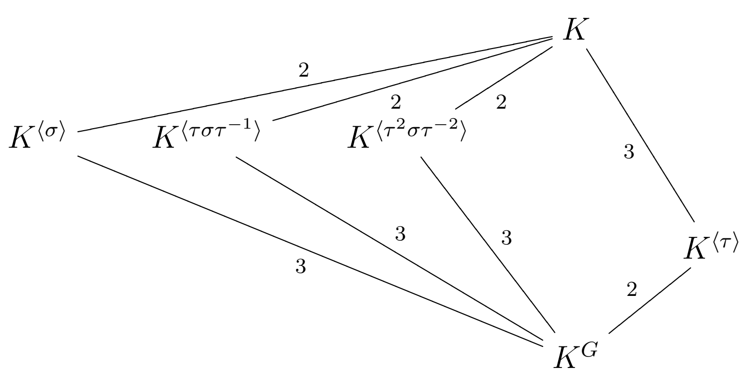
We know, from the Fundamental Theorem of Galois Theory, that $\dim_{K^G} K = |G| = 6$. Suppose $g \in K^G$ and $f(x) \in (\boldsymbol{k}[g])[x]$, with $f(t) = 0$, then

$$6 = \dim_{K^G} K \leq \dim_{\boldsymbol{k}[g]} K = \dim_{\boldsymbol{k}[g]} (\boldsymbol{k}[g])[t] \leq \deg f$$

We already addressed the left-most equality. The left-most inequality holds because $\boldsymbol{k}[g] \subseteq K^G$. The middle equality holds because $K = (\boldsymbol{k}[g])[t]$. The right-most inequality holds because the minimal polynomial of t over $\boldsymbol{k}[g]$ divides into f. If f has degree larger than 6, then we do not learn anything; however, if f has degree 6, then equality holds across the board and $\boldsymbol{k}[g] = K^G$. Indeed,

$$\dim_{K^G} K = \dim_{\boldsymbol{k}[g]} K = \dim_{\boldsymbol{k}[g]} K^G \dim_{K^G} K \implies \dim_{\boldsymbol{k}[g]} K^G = 1.$$

Our job is to find $g \in K^G$ and $f \in (\boldsymbol{k}[g])[x]$ such that $f(t) = 0$ and $\deg f = 6$. We start by finding elements of K^G. Of course, the intermediate fields are



It is clear that $r_1 = t + \sigma(t)$ is in $K^{\langle\sigma\rangle}$. (I probably could check that r_1 is not in K^G; but I am not going to make that check publicly. I am just going to assume it is true. If I am right, I will get what I need. If I am wrong, I won't get anywhere and I will have to start over.) If $K^{\langle\sigma\rangle} = K^G[r_1]$, as I strongly suspect, then $K^{\langle\tau\sigma\tau^{-1}\rangle} = K^G[r_2]$ and $K^{\langle\tau^2\sigma\tau^{-2}\rangle} = K^G[r_3]$ for

$$r_2 = \tau r_1 \quad \text{and} \quad r_3 = \tau^2 r_1.$$

I assume that

$$(x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3$$

is the minimal polynomial of r_1 over K^G. I am certain that

$$r_1 + r_2 + r_3,\ r_1r_2 + r_1r_3 + r_2r_3,\ \text{and } r_1r_2r_3$$

are elements of K^G. Now might be a good time to write down what these r's are. Let

$$r_1 = t + \sigma(t) = t + 1/t, \quad r_2 = \tau(r_1) = \frac{t-1}{t} + \frac{t}{t-1}, \quad \text{and}$$

$$r_3 = \tau^2(r_1) = \frac{1}{1-t} + 1 - t.$$

The sum $r_1 + r_2 + r_3$ is not very interesting. (It is two.) I am going to pick on $r_1r_2 + r_1r_3 + r_2r_3$. When I write this expression as a rational function in $\boldsymbol{k}(t)$, it will look like

$$\frac{p(t)}{q(t)},$$

where $p(t)$ and $q(t)$ are in $\boldsymbol{k}[t]$. I expect $\deg p = 6$ and $\deg q = 4$. If I let $g = \frac{p(t)}{q(t)}$, then I know that $g \in K^G$ and

$$f(x) = p(x) - gq(x)$$

is a polynomial of degree six in $K^G[x]$ and I also know that $f(t)$, which is equal to $p(t) - gq(t)$, is zero.

Let's express $r_1r_2 + r_1r_3 + r_2r_3$ as a rational function in t. I have to make sure that it doesn't simplify to become something inappropriate (like $r_1 + r_2 + r_3$ did.) I got maple to help.

Activities   Document Viewer   Sat Mar 30, 11:16 PM

3 of 5   scrap.pdf   200%

```
> r_1:=t+1/t;
                                       r_1 := t + 1/t

> r_2:=(t-1)/t+t/(t-1);
                                           t - 1     t
                                    r_2 := ----- + -----
                                             t     t - 1

> r_3:=1/(1-t)+ 1-t;
                                             1
                                    r_3 := ----- + 1 - t
                                           1 - t

> g:=r_1*r_2+r_1*r_3+r_2*r_3;
               /t - 1     t  \             /  1          \   /t - 1     t  \ /  1          \
g := (t + 1/t) |----- + -----| + (t + 1/t) |----- + 1 - t| + |----- + -----| |----- + 1 - t|
               \  t     t - 1/             \1 - t        /   \  t     t - 1/ \1 - t        /

> simplify (g);
                              6      5      4    3      2
                            -t  + 3 t  - 3 t  + t  - 3 t  + 3 t - 1
                            ---------------------------------------
                                           2        2
                                          t  (t - 1)

>
```

Plain Text   Tab Width: 8   Ln 25, Col 1

So,

$$g = \frac{-t^6 + 3t^5 - 3t^4 + t^3 - 3t^2 + 3t - 1}{t^2(t-1)^2},$$
$$t^2(t-1)^2 g = -t^6 + 3t^5 - 3t^4 + t^3 - 3t^2 + 3t - 1,$$

and

$$f(x) = -x^6 + 3x^5 - 3x^4 + x^3 - 3x^2 + 3x - 1 - x^2(x-1)^2 g$$

is a polynomial of degree 6 in $K^G[x]$ with $f(t) = 0$. We conclude that $\boldsymbol{k}[g] = K^G$ for

$$g = \frac{-t^6 + 3t^5 - 3t^4 + t^3 - 3t^2 + 3t - 1}{t^2(t-1)^2}.$$

17. Let $\boldsymbol{k}$ be a field of characteristic p and let $f(x) = x^p - x - a \in \boldsymbol{k}[x]$. Suppose that $f(x) = 0$ has no solution in $\boldsymbol{k}$. Let K be a splitting field of $f(x)$ over $\boldsymbol{k}$. Is $\boldsymbol{k} \subseteq K$ a Galois extension? Find $\operatorname{Aut}_{\boldsymbol{k}} K$.

Let $\alpha \in K$ be a solution of $f(x) = 0$. It is now clear that the complete solution set is

$$\{\alpha + j \mid 0 \le j \le p-1\}.$$

Thus, $K = \boldsymbol{k}[\alpha]$ and K is the splitting field of a separable polynomial over $\boldsymbol{k}$. Thus, $\boldsymbol{k} \subseteq K$ is a Galois extension. Observe that $f(x)$ is irreducible over $\boldsymbol{k}$ because any factor of $f(x)$ over $\boldsymbol{k}$, has the form

$$(x - [\alpha + j_1]) \cdots (x - [\alpha + j_m]) = x^m - (m\alpha + j_1 + \cdots + j_m)x^{m-1} + \ldots$$

for some distinct $j_1, \ldots, j_m$ with $0 \le j_k \le p-1$. If the above factor of $f(x)$ is in $\boldsymbol{k}[x]$, with $1 \le m \le p-1$, then $m\alpha + j_1 + \cdots + j_m \in \boldsymbol{k}$; so $m\alpha \in \boldsymbol{k}$; so $\alpha \in \boldsymbol{k}$ and this contradicts the assumption.

The elements α and $\alpha + 1$ of K have the same minimal polynomial, so there is an automorphism of K over $\boldsymbol{k}$ which is defined by $\sigma(\alpha) = \alpha + 1$. It is clear that σ has order p in $\operatorname{Aut}_{\boldsymbol{k}} K$. On the other hand, $|\operatorname{Aut}_{\boldsymbol{k}} K| = \dim_{\boldsymbol{k}} K = p$. We conclude that $\operatorname{Aut}_{\boldsymbol{k}} K$ is the cyclic group of order p, which is generated by σ.

18. **Give an example of a finite dimensional field extension $\boldsymbol{k} \subseteq K$ with an infinite number of intermediate fields. Also give an example of a finite dimensional field extension $\boldsymbol{k} \subseteq K$ with $K \neq \boldsymbol{k}[u]$ for any $u \in K$.**

Let $\boldsymbol{\ell}$ be an infinite field of characteristic p for some prime integer p. (For example, $\boldsymbol{\ell}$ could be the field of rational functions in one variable over $\frac{\mathbb{Z}}{(p)}$.) Let $\boldsymbol{k} = \boldsymbol{\ell}(s^p, t^p)$ and $K = \boldsymbol{\ell}(s, t)$. (In particular, $\boldsymbol{k}$ and K are both fields of rational functions in two variables.) Observe that $x^p - s^p$ is an irreducible polynomial in $\boldsymbol{k}[x]$. (See, for example, Example 5.37.(b) from the class notes.) Thus,

$$\dim_{\boldsymbol{k}} \boldsymbol{k}(s) = p.$$

In a similar manner, $\dim_{\boldsymbol{\ell}(s,t^p)} K = p$. We conclude that $\dim_{\boldsymbol{k}} K = p^2$. We first prove that K is not equal to $\boldsymbol{k}(u)$ for any u in K. Indeed, if $u \in K$, then $u^p \in \boldsymbol{k}$ and

$$\dim_{\boldsymbol{k}} \boldsymbol{k}(u) \le p < p^2 = \dim_{\boldsymbol{k}} K.$$

Observe that for each $\alpha \in \boldsymbol{\ell}$, $\boldsymbol{k}(s+\alpha t)$ is a field with

$$\boldsymbol{k} \subseteq \boldsymbol{k}(s+\alpha t) \subseteq K.$$

Claim. *All of the intermediate fields $\boldsymbol{k}(s+\alpha t)$ are distinct as α ranges over the infinite set $\boldsymbol{\ell}$.*

To prove the claim, we assume α and β are distinct elements of the field $\boldsymbol{\ell}$ and

$$\boldsymbol{k}(s+\alpha t) = \boldsymbol{k}(s+\beta t).$$

We look for a contradiction. Thus

$$(\alpha-\beta)t = (s+\alpha t) - (s+\beta t) \in \boldsymbol{k}(s+\alpha t).$$

But, $\alpha-\beta$ is a unit of $\boldsymbol{k}$; hence t (and therefore s and K) are in $\boldsymbol{k}(s+\alpha t)$. We already proved that $K \neq \boldsymbol{k}(u)$ for any u. We have reached a contradiction. The Claim is established.