Math 6122: HW 4

Due: Thursday, February 7th, start of class

Let $\chi_1, \ldots, \chi_n$ be pairwise distinct homomorphisms from a group G to the multiplicative group $F^\times$ of nonzero elements of a field F. **Dedekind's lemma on linear independence of characters** states that $\chi_1, \ldots, \chi_n$ are linearly independent elements of the F-vector space $\mathrm{Fun}(G, F)$, i.e., if

$$a_1\chi_1 + \ldots + a_n\chi_n = 0 \in \mathrm{Fun}(G, F),$$

for some $a_i \in F$, then $a_i = 0$ for all i.

There is a short and easy proof of this lemma – it's a proof by contradiction using the length of a minimal dependence relation, and the fact that for a fixed h the map $g \mapsto gh$ permutes the elements of G. Try it! (Or read Section 14.2, Theorem 7).The textbook gives a different proof of the main theorem of Galois theory using this lemma in Section 14.2, which you may read if you wish.

You may assume the statement of Dedekind's lemma for the following problems (Problems 22,23,25,26 from Section 14.2 in Dummit and Foote. See the book for hints).

In the following problems, let K/F be a Galois extension with Galois group G. Define the norm and trace maps $\mathrm{N}_{K/F} \colon K \to F$ and $\mathrm{Tr}_{K/F} \colon K \to F$ by

$$\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha),$$

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

1. - Suppose $\alpha \in K$ is of the form $\alpha = \beta/\sigma(\beta)$ for some nonzero $\beta \in K$. Prove that $\mathrm{N}_{K/F}(\alpha) = 1$.
   - Suppose $\alpha \in K$ is of the form $\alpha = \beta - \sigma(\beta)$ for some $\beta \in K$. Prove that $\mathrm{Tr}_{K/F}(\alpha) = 0$.

2. (Hilbert's Theorem 90) Assume that G is cyclic. Suppose $\alpha \in K$ has $\mathrm{N}_{K/F}(\alpha) = 1$. Prove that α is of the form $\alpha = \beta/\sigma(\beta)$ for some nonzero $\beta \in K$.

3. Use Hilbert's Theorem 90 to prove that the rational solutions (a, b) to the equation $a^2 + Db^2 = 1$ for some nonsquare integer $D > 0$ are of the form $a = \frac{s^2 - Dt^2}{s^2 + Dt^2}$ and $b = \frac{2st}{s^2 + Dt^2}$. [Hint: Take $K = \mathbb{Q}(\sqrt{-D})$.]

4. (Additive Hilbert's Theorem 90) Assume that G is cyclic. Suppose $\alpha \in K$ has $\mathrm{Tr}_{K/F}(\alpha) = 0$. Prove that α is of the form $\alpha = \beta - \sigma(\beta)$ for some $\beta \in K$.

Math 6122 - Homework 4

Caitlin Beecham (Discussed with)

February 7, 2019

1

We compute the following.

$$\begin{aligned}
N_{K/F}(\alpha) &= \prod_{\sigma \in G} \sigma(\alpha) \\
&= \prod_{\sigma \in G} \sigma(\frac{\beta}{\tilde{\sigma}(\beta)}) \\
&= \prod_{\sigma \in G} \sigma(\beta) \prod_{\sigma \in G} \sigma(\frac{1}{\tilde{\sigma}(\beta)}) \\
&= \frac{\prod_{\sigma \in G} \sigma(\beta)}{\prod_{\sigma \in G} \sigma(\tilde{\sigma}(\beta))} \\
&= \frac{\prod_{\sigma \in G} \sigma(\beta)}{\prod_{\sigma \in G} \sigma(\beta)} \\
&= 1
\end{aligned}$$

Additionally, we compute the following.

$$\begin{aligned}
Tr_{K/F}(\alpha) &= \sum_{\sigma \in G} \sigma(\alpha) \\
&= \sum_{\sigma \in G} \sigma(\beta - \tilde{\sigma}(\beta)) \\
&= \sum_{\sigma \in G} \sigma(\beta) - \sum_{\sigma \in G} \sigma(\tilde{\sigma}(\beta)) \\
&= \sum_{\sigma \in G} \sigma(\beta) - \sum_{\sigma \in G} \sigma(\beta) \\
&= 0
\end{aligned}$$

2

We first show that there exists some $\theta \in K$ such that

$$\beta = \theta + \alpha\sigma(\theta) + (\alpha\sigma(\alpha))\sigma^2(\theta) + (\alpha\sigma(\alpha)\sigma^2(\alpha))\sigma^3(\theta) + \cdots + (\alpha\sigma(\alpha)\sigma^2(\alpha)\ldots\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta) \tag{1}$$

is non-zero.
To do so, we note that the homomorphisms $\chi_i : E^\times \to E^\times$ defined by $\chi_i(\theta) = \sigma^i(\theta)$ for $i \in [n-1]$ and $\chi_0 = \text{id}$. Then, by linear independence of characters and the fact that $b_0 = 1 \neq 0$, we have that

$$\sum_{i=0}^{n} b_i\chi_i = \sum_{i=0}^{n}((\prod_{j=1}^{i}\sigma^{i-1}(\alpha))\chi_i) \tag{2}$$

$$\tag{3}$$

Now, since b_i are not all identically zero, the above function from $E^\times \to E$ is not the zero function. Therefore, our desired θ exists.
Finally, we note that

$$\begin{aligned}\sigma(\beta) &= \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) && (4)\\ &+ \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha)\sigma^4(\theta) + \cdots + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha)\ldots\sigma^{n-1}(\alpha)\theta && (5)\\ &= \frac{1}{\alpha}\beta && (6)\end{aligned}$$

So, we get that $\alpha = \frac{\beta}{\sigma(\beta)}$.

3

We note that $a^2 + Db^2 = 1$ is equivalent to saying that $N_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(a - b\sqrt{-D}) = 1$. So, we know that $a + b\sqrt{-D}$ is of the form $a + b\sqrt{-D} = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in \mathbb{Q}(\sqrt{-D})$ and some $\sigma \in Gal(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$. Now, we have two cases. Either σ is the identity map or not. If so, then $a + b\sqrt{-D} = 1$ which means that $a = \frac{s^2-Dt^2}{s^2+Dt^2}$ and $b = \frac{2st}{s^2+Dt^2}$ with $s = 1$ and $t = 0$. Now, say σ is not the identity map. Then, we know $a + b\sqrt{-D} = \frac{\alpha+f\sqrt{D}i}{\alpha-f\sqrt{D}i} = \frac{\alpha^2-f^2D+2\alpha f\sqrt{D}i}{\alpha^2+f^2D}$, which means that $a = \frac{\alpha^2-f^2D}{\alpha^2+f^2D}$ and $b = \frac{2\alpha f}{\alpha^2+f^2D}$

4

Lemma:
We use linear independence of characters to show that there exists some $\theta \in E$ with $Tr_{E/F}(\theta) \neq 0$. Let $\chi_i := \sigma_i$ where the Galois group $G = \{\sigma_i | i \in [n]\}$. Next, consider the linear combination $\sum_{i=1}^{n} \chi_i$. We note that since the coefficients of this sum are not identically zero, this function is not the zero function. So, there exists some $\theta \in E$ such that $Tr_{E/F}(\theta)$.
Now, let $\beta = \frac{1}{Tr_{E/F}(\theta)}[\alpha\sigma(\theta)+(\alpha+\sigma(\alpha))\sigma^2(\theta)+\cdots+(\alpha+\sigma(\alpha)+\cdots+\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta)]$. Next, we compute $\sigma(\beta) = \frac{1}{Tr_{E/F}(\theta)}[\sigma(\alpha)\sigma^2(\theta)+(\sigma(\alpha)+\sigma^2(\alpha))\sigma^3(\theta)+\cdots+(\sigma(\alpha)+\sigma^2(\alpha)+\cdots+\sigma^{n-1}(\alpha))\theta]$ and finally note that $\alpha = \beta - \sigma(\beta)$.