Math 30820 Honors Algebra 4
Homework 13

Andrei Jorza

Due Wednesday, 5/3/2017

Do 4 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

1. Let K/F be a finite Galois extension, $\sigma \in \mathrm{Gal}(K/F)$ and $x \in K^\times$.

   (a) Show that $N_{K/F}(x/\sigma(x)) = 1$.

   (b) Show that $\mathrm{Tr}_{K/F}(x - \sigma(x)) = 0$.

   Proof. First, if $\sigma \in G = \mathrm{Gal}(K/F)$ then $\{g\sigma \mid g \in G\} = G$. Therefore $\mathrm{Tr}(\sigma(\alpha)) = \sum g\sigma(\alpha) = \sum g(\alpha) = \mathrm{Tr}(\alpha)$ and similarly for the norm. Finally, the results follows from additivity for the trace and multiplicativity for the norm. □

2. Suppose K/F is a finite Galois extension with $\mathrm{Gal}(K/F)$ cyclic of order n generated by an automorphism σ. Show that if $\alpha \in K$ has the property $\mathrm{Tr}_{K/F}(\alpha) = 0$ then there exists $\beta \in K$ such that $\alpha = \beta - \sigma(\beta)$. [Hint: Similarly to the theorem from class, look at

$$\frac{1}{\mathrm{Tr}_{K/F}(\theta)} \sum_{i=1}^{n-1} \sigma^i(\theta) \sum_{j=0}^{i-1} \sigma^j(\alpha)$$

   for suitably chosen θ.]

   Proof. From class we can choose θ such that $\mathrm{Tr}(\theta) \neq 0$ and we denote by β the expression in the hint, which now makes sense. We compute (using $\mathrm{Tr}(\theta) \in F$)

$$\begin{aligned} \sigma(\beta) &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{i=1}^{n-1} \sigma^{i+1}(\theta) \sum_{j=0}^{i-1} \sigma^{j+1}(\alpha) \\ &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{i=2}^{n} \sigma^{i}(\theta) \sum_{j=0}^{i-2} \sigma^{j+1}(\alpha) \\ &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{i=2}^{n} \sigma^{i}(\theta) \sum_{j=1}^{i-1} \sigma^{j}(\alpha) \end{aligned}$$

Since $\sigma^n(\alpha) = \alpha$ as σ has order n this expression is

$$\begin{aligned}
\sigma(\beta) &= \frac{1}{\mathrm{Tr}(\theta)} \left(\sum_{i=2}^{n-1} \sigma^i(\theta) \sum_{j=1}^{i-1} \sigma^j(\alpha) + \theta \sum_{j=1}^{n-1} \sigma^j(\alpha) \right) \\
&= \frac{1}{\mathrm{Tr}(\theta)} \left(\sum_{i=2}^{n-1} \sigma^i(\theta) \sum_{j=1}^{i-1} \sigma^j(\alpha) + \theta(\mathrm{Tr}(\alpha) - \alpha) \right) \\
&= \frac{1}{\mathrm{Tr}(\theta)} \left(\sum_{i=1}^{n-1} \sigma^i(\theta) \sum_{j=1}^{i-1} \sigma^j(\alpha) - \theta\alpha \right) \\
&= \frac{1}{\mathrm{Tr}(\theta)} \left(\sum_{i=1}^{n-1} \sigma^i(\theta) \sum_{j=0}^{i-1} \sigma^j(\alpha) - \sum_{i=1}^{n-1} \sigma^i(\theta)\alpha - \theta\alpha \right) \\
&= \beta - \frac{1}{\mathrm{Tr}(\theta)} \left(\sum_{i=1}^{n-1} \sigma^i(\theta)\alpha + \theta\alpha \right) \\
&= \beta - \frac{1}{\mathrm{Tr}(\theta)} \mathrm{Tr}(\theta)\alpha \\
&= \beta - \alpha
\end{aligned}$$

as $\mathrm{Tr}(\alpha) = 0$ and $\sum_{j=1}^{i-1}$ is the empty sum when $i = 1$. □

3. Let $a, b \in \mathbb{Z}$. Find all $(x, y) \in \mathbb{Q}^2$ such that $x^2 + axy + by^2 = 1$.

   Proof. Rewrite the equation as
   $$(x + ay/2)^2 - \Delta(y/2)^2 = 1$$
   where $\Delta = a^2 - 4b$. Denote $u = x + ay/2$ and $v = y/2$ which yield $y = 2v$ and $x = u - ay/2 = u - av$. Therefore it suffices to solve $u^2 - \Delta v^2 = 1$ in $\mathbb{Q}$.

   Let $K = \mathbb{Q}(\sqrt{\Delta})$. If Δ is a square in $\mathbb{Q}$ then $\Delta = d^2$ and the equation becomes $u^2 - d^2v^2 = 1$ so $(u - dv)(u + dv) = 1$. If $d = 0$ then $u^2 = 1$ which yields $u = \pm 1$ and anything for v. If $d \neq 0$ then for any $t \in \mathbb{Q}^\times$ we get a solution to $u - dv = t$ and $u + dv = 1/t$ with $u = (t + 1/t)/2$ and $v = (u - t)/d$.

   If Δ is not a square in $\mathbb{Q}$ then $K/\mathbb{Q}$ is Galois with quadratic Galois group $\{a + b\sqrt{\Delta} \mapsto a \pm b\sqrt{\Delta}\}$, with σ the unique nontrivial automorphism. Then from class $N_{K/\mathbb{Q}}(u + v\sqrt{\Delta}) = u^2 - \Delta v^2$ so $u^2 - \Delta v^2 = 1$ if and only if $N_{K/\mathbb{Q}}(u + v\sqrt{\Delta}) = 1$. Hilbert 90 implies this happens if and only if
   $$u + v\sqrt{\Delta} = \frac{a + b\sqrt{\Delta}}{a - b\sqrt{\Delta}} = \frac{a^2 + \Delta b^2}{a^2 - \Delta b^2} + \frac{2ab\sqrt{\Delta}}{a^2 - \Delta b^2}$$
   for some $a, b \in \mathbb{Q}$. This yields all the solutions. □

4. (Correction of Artin 16.M.11.(c)) Keep the notations from 16.M.11. Prove that if $\gamma \neq 0$ then $\delta\gamma \in F$ if and only if $G = C_4$. Similarly, prove that if $\varepsilon \neq 0$ then $\delta\varepsilon \in F$ if and only if $G = C_4$.

   Proof. Recall that $\sigma(\delta) = \varepsilon(\sigma)\delta$ so $\delta\gamma \in F$ (respectively $\delta\varepsilon \in F$) iff $\sigma(\gamma) = \varepsilon(\sigma)\gamma$ (respectively $\sigma(\varepsilon) = \varepsilon(\sigma)\varepsilon$) for all $\sigma \in G$. Since $(12) \in H$ fixes γ and ε it follows that $\delta\gamma \in F$ (respectively $xh\varepsilon \in F$), when nonzero, if and only if $(12) \notin G$, i.e., iff $G = C_4$. □

5-6 (Worth 2 problems) Let $L/K/F$ be finite extensions such that L/F is Galois. Write $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$ and let $\{\sigma_1, \ldots, \sigma_n\}$ be a complete set of representatives in G of G/H, i.e., $G/H = \{\sigma_1 H, \ldots, \sigma_n H\}$. For $\alpha \in K$ define

$$\mathcal{P}_{\alpha,L}(X) = \prod_{\sigma \in \mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K)} (X - \sigma(\alpha)) = \prod_{i=1}^{n} (X - \sigma_i(\alpha))$$

(a) Show that $\mathcal{P}_{\alpha,L}(X)$ is a well-defined polynomial with coefficients in F. (Careful: K/F need not be Galois.)

(b) Define $\mathrm{Tr}_{K/F,L}(\alpha)$ and $N_{K/F,L}(\alpha)$ as the coefficients of $\mathcal{P}_{\alpha,L}(X)$ as follows:

$$\mathcal{P}_{\alpha,L}(X) = X^n - \mathrm{Tr}_{K/F,L}(\alpha) X^{n-1} + \cdots + (-1)^n N_{K/F,L}(\alpha)$$

Show that $\mathrm{Tr}_{K/F,L} : K \to F$ is a homomorphism of F-vector spaces and $N_{K/F,L} : K^\times \to F^\times$ is a group homomorphism.

(c) If L'/L is a finite extension such that L'/F is Galois show that $\mathcal{P}_{\alpha,L}(X) = \mathcal{P}_{\alpha,L'}(X)$.

(d) Deduce that $\mathcal{P}_{\alpha,L}(X)$ (and therefore also $\mathrm{Tr}_{K/F,L}$ and $N_{K/F,L}$) does not depend on the choice of Galois extension L/F. (We can therefore drop the subscript L from notation to obtain trace $\mathrm{Tr}_{K/F}$ and norm $N_{K/F}$ for all finite extensions.)

Proof. (a): Note that $\mathrm{Gal}(L/K)$ fixes α so the expression is well-defined, independent of choices of coset representatives. As in class it suffices to check that $\mathcal{P}_{\alpha,L}(X) \in L[X]^{\mathrm{Gal}(L/F)}$. Let $g \in \mathrm{Gal}(L/F)$. For each σ_i, the automorphism $g\sigma_i$ lands in one of the cosets $\sigma_j H$ and write $g\sigma_i = \sigma_{j(g,i)} h_{g,i}$ for some index $j(g,i)$ and some $h_{g,i} \in H$. Note that if $j(g,i) = j(g,i')$ then $g\sigma_i H = g\sigma_{i'} H$ which would imply that $\sigma_i H = \sigma_{i'} H$.

Then

$$\begin{aligned} g(\mathcal{P}_{\alpha,L}(X)) &= \prod (X - g\sigma_i(\alpha)) \\ &= \prod (X - \sigma_{j(g,i)} h_{g,i}(\alpha)) \\ &= \prod (X - \sigma_{j(g,i)}(\alpha)) \\ &= \mathcal{P}_{\alpha,L}(X) \end{aligned}$$

as $\{\sigma_{j(g,i)}\} = \{\sigma_i\}$ since all the indices $j(g,i)$ are distinct as i varies.

(b): Follows from the additivity and multiplicativity of each σ_i.

(c): Consider the tower $L' - L - K - F$ and write $G' = \mathrm{Gal}(L'/K)$, $H' = \mathrm{Gal}(L'/K)$ and $N = \mathrm{Gal}(L'/L)$. From the main theorem N is normal in G' as L/F is Galois. Moreover, from the main theorem and the third isomorphism theorem we get

$$G/H \cong (G'/N)/(H'/N) \cong G'/H'$$

and therefore in the defining expression for $\mathcal{P}_{\alpha,L'}$ we may choose representatives $\sigma_i \in \mathrm{Gal}(L'/F)$ that correspond to the representatives $\sigma_i \in \mathrm{Gal}(L/F)$ under the previous isomorphism. The defining expressions for $\mathcal{P}_{\alpha,L}$ and $\mathcal{P}_{\alpha,L}$ are the same as the third isomorphism theorem map takes the coset representative $\sigma \in \mathrm{Gal}(L'/F)$ to $\sigma \mod N \in \mathrm{Gal}(L/F)$ and $N \subset \mathrm{Gal}(L'/K)$ fixes α.

(d): Let L, L' be two different Galois extensions of F containing K. Let E/F be a Galois extension containing the composite LL'. Then the previous part shows that

$$\mathcal{P}_{\alpha,L}(X) = \mathcal{P}_{\alpha,E}(X) = \mathcal{P}_{\alpha,L'}(X)$$

as desired. □