Algebra II, Spring 2017

Solutions to Problem Set 4

1. (a) Let $f(x)$ be the minimal polynomial of α over F and $p(x)$ its characteristic polynomial, $p(x) = \det(xI - L_\alpha)$. Then $T(\alpha)$ is the sum of roots of $p(x)$. On the other hand, we have seen in class that $p(x) = f(x)^{[E:F(\alpha)]}$, and for every root β of $f(x)$, there are exactly $[E : F(\alpha)]$ automorphisms which send α to β. So if $\alpha = \alpha_1, \dots, \alpha_n$ are the roots of $f(x)$, then the sum of roots of $p(x)$ is exactly

$$\sum_{\sigma \in G} \sigma(\alpha)$$

so we get the desired equality.

(b) Let $G = \{\sigma_1, \dots, \sigma_k\}$. Then each σ_i is a character $E^\times \to E^\times$. So by the theorem on independence of characters, a linear combination of the σ_i is identically equal to zero only if all the coefficients are zero. Apply this to the linear combination $\sigma_1 + \cdots + \sigma_k$.

2. Let $|G| = n$. It is clear by part (a) of Question 1 that $T(\sigma(\alpha)) = T(\alpha)$, so $\beta - \sigma(\beta)$ is in the kernel of T for every β. Assume now that α is in the kernel of T. Follow the same method to prove the multiplicative version of Hilbert's Theorem 90: by part (b) of Question 1, there is $x \in E$ such that $x + \sigma(x) + \cdots + \sigma^{n-1}(x) = T(x) \neq 0$. Now let

$$\gamma = c_0 x + c_1 \sigma(x) + \cdots + c_{n-1}\sigma^{n-1}(x)$$

where $c_i = \alpha + \sigma(\alpha) + \cdots + \sigma^i(\alpha)$. So $\sigma(c_i) = c_{i+1} - \alpha$ for $0 \le i \le n-1$ (we let $c_n := c_0 = \alpha$.) Then

$$\sigma(\gamma) - \gamma = \sum_{i=0}^{n-1} (\sigma(c_i) - c_{i+1})\sigma^{i+1}(x) = -\alpha T(x).$$

But since $T(x) \in F$, and is nonzero, if we set $\beta = \frac{-\gamma}{T(x)}$, we get

$$\sigma(\beta) - \beta = \alpha.$$

3. (a) In a field of characteristic p, $(a+b)^p = a+b$. Also if $\mathbf{F}_p \subset F$, and if $j \in \mathbf{F}_p$, then $j^p = j$. So if $\alpha^p - \alpha - x = 0$, then $(\alpha+j)^p - (\alpha+j) - c = \alpha^p + j^p - \alpha - j - c = j^p - j = 0$. Since $f(x)$ has at most p distinct roots, every root should be of the form $\alpha + j$ for some $0 \leq j \leq p-1$.

(b) Let G be generated by σ. Note that for any $c \in F$, by part (a) of Question 1, $T(c) = p\,c = 0$, in particular $T(1) = 0$. So By Question 2, there is $\beta \in L$ such that

$$1 = \beta - \sigma(\beta).$$

Therefore $\sigma(\beta) = \beta + 1$, and so $\sigma^i(\beta) = \beta + i$ for every $0 \leq i \leq p-1$. So if $f(x)$ is the minimal polynomial of β, then $\beta + i$ is a root of $f(x)$ for every $0 \leq i \leq p-1$. If $m = \deg f(x)$, then $m = [F(\alpha) : F] \leq [L : F] = p$, so $m = p$, $L = F(\beta)$, and the set of roots of f is $\{\beta, \beta+1, \ldots, \beta+(p-1)\}$. It remains to show $\beta^p - \beta \in F$. We show $\beta^p - \beta$ is the fixed field of G: for every $\rho \in G$, $\rho = \sigma^i$ for some $0 \leq i \leq p-1$, so

$$\rho(\beta^p - \beta) = \rho(\beta)^p - \rho(\beta) = (\sigma^i(\beta))^p - \sigma^i(\beta) = (\beta+i)^p - (\beta+i) = \beta^p + i^p - \beta - i = \beta^p - \beta.$$

4. Suppose that

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

is a tower which satisfies the two given properties: f splits in F_m and $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in F_{i-1}$. Let f_i be the minimal polynomial of α_i over F and let L_i be the splitting field of $f_1 f_2 \ldots f_i$. Then we have a tower

$$F \subset L_1 \subset \cdots \subset L_m$$

where each L_i is Galois over F, and f splits in L_m. So it is enough to show we can refine the inclusion $L_{i-1} \subset L_i$ to get a tower of field extensions such that each is obtained from the previous one by adding a root of an element. Let $\alpha_i = \beta_1, \beta_2, \ldots \beta_{m_i}$ be the roots of the polynomial f_i. We have a tower

$$L_{i-1} \subset L_{i-1}(\beta_1) \subset \cdots \subset L_{i-1}(\beta_1, \ldots, \beta_{m_i}) = L_i.$$

Note that for each β_j, $1 \leq j \leq m_i$, there is an automorphism $\sigma \in \mathrm{Gal(L_m/F)}$ such that $\sigma(\alpha_i) = \beta_j$ (since $\alpha_i = \beta_1$ and β_j are roots of the same irreducible polynomial in $F[x]$). Since $\alpha_i^{n_i} \in F_{i-1}$ by our original assumption, and since $F_{i-1} \subset L_{i-1}$ (by definition), $\beta_j^{n_i} = \sigma(\alpha_i^{n_i}) \in \sigma(F_{i-1}) \subset \sigma(L_{i-1})$. Since L_{i-1} is Galois over F, σ sends elements of L_{i-1} to elements of L_{i-1}, hence $\beta_j^{n_i} \in L_{i-1} \subset L(\beta_1, \ldots, \beta_{j-1})$.

5. If we consider the quadratic extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{-d})$, then we have the norm map

$$N(a + b\sqrt{-d}) = a^2 + db^2,$$

so we are looking for all elements $x + y\sqrt{-d}$ with norm 1. By Hilbert theorem 90, they are of the form $x+y\sqrt{-d} = \frac{\sigma(\beta)}{\beta}$ for some $\beta = m+n\sqrt{-d}$ where $\sigma(m+n\sqrt{-d}) = m - n\sqrt{-d}$. So

$$x + y\sqrt{-d} = \frac{m - n\sqrt{-d}}{m + n\sqrt{-d}} = \frac{m^2 - dn^2 - 2mn\sqrt{-d}}{m^2 + dn^2} = \frac{m^2 - dn^2}{m^2 + dn^2} + \frac{-2mn}{m^2 + dn^2}\sqrt{-d}.$$

so

$$x = \frac{m^2 - dn^2}{m^2 + dn^2}, \quad y = \frac{-2mn}{m^2 + dn^2}$$

for rational numbers m, n.