Algebra IIR, list 5.

Homework: as usual. Items and problems marked with $-$ are excluded from homework.

1. Assume that $char(K) = p > 0$, $K \subset L$ is an algebraic field extension and $a \in L \setminus K$. Prove that a^{p^l} is separable over K for some $l \geqslant 0$.

2. Let $K \subset L \subset M \subset \hat{K}$, $[M : K] < \infty$ i $a \in L$. Prove that
(a) $Tr_{M/K}(a) = [M : L] \cdot Tr_{L/K}(a)$,
(b) $N_{M/K}(a) = N_{L/K}(a)^{[M:L]}$,
(c) $Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}$,
(d) $N_{M/K} = N_{L/K} \circ N_{M/L}$.

3. Assume that $a \in L$ is algebraic over K, $L = K[a]$ and $W(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ is the minimal polynomial of a over K. Prove (directly from definition) that
(a) $Tr_{L/K}(a) = -a_{n-1}$,
(b) $N_{L/K}(a) = (-1)^n a_0$,
(c) $W(X) = (-1)^n\varphi(x)$, where $\varphi(x)$ is the characteristic polynomial of the linear transformation $f_a : L \to L$.

4. (a) Prove that Frobenius automorphism $\varphi_n(x) = x^p$ is a generator of the group $G(F(p^n)/F(p))$.
(b) For $m|n$, $F(p) \subset F(p^m) \subset F(p^n)$. Let $\Phi : G(F(p^n)/F(p)) \to G(F(p^m)/F(p))$ be restriction to $F(p^n)$. Point out a generator of the group $Ker(\Phi) = G(F(p^n)/F(p^m))$.
(c)* Point out an element $g \in G(\widehat{F(p)}/F(p))$ that is not a power of the Frobenius automorphism. Prove that $Aut(\widehat{F(p)})$ has power $2^{\aleph_0}$.

5. Assume that $K \subseteq L_1, L_2 \subseteq \hat{K}$ and $K \subseteq L_i$ are (finite) Galois extensions.
(a)– Prove that the extension $K \subseteq L_1 \cdot L_2$ is Galois.
(b) Prove that if $G(L_1/K)$ and $G(L_2/K)$ are Abelian, then $G(L_1L_2/K)$ is also Abelian.
(c) Assume $L_1 \cap L_2 = K$. Prove that $G(L_1L_2/L_1) \cong G(L_2/K)$[1]
(d) Assume $L_1 \cap L_2 = K$. Prove that $G(L_1L_2/K) \cong G(L_1/K) \times G(L_2/K)$.

6. Prove that every finite group G is isomorphic to the Galois group of some Galois extension.[2]

7. (a) Assume that L is a finite extension of the field $\mathbb{Q}$, of odd degree. Prove that L is isomorphic over $\mathbb{Q}$ with a subfield of the field $\mathbb{R}$.

[1]Hint: consider restriction to L_2. Use connection between the order of Galois group and the degree of Galois extension.

[2]Hint: By the Cayley Thm we may assume that $G < Sym(\{X_1, \ldots, X_n\})$ for some n. Consider the field $K(X_1, \ldots, X_n)$.

(b)– Prove that every finite extension $L \supset \mathbb{R}$ has degree being a power of 2. [3]
(c)– Prove that $\mathbb{C}$ is algebraically closed.[4]

8. * Prove that every finite Abelian group is the Galois group of some Galois extension of $\mathbb{Q}$ (it is an open problem, if it is true for any finite group, not necessarily Abelian).[5]

9. – Assume that A is an algebraic structure, $H < Aut(A)$ and $f \in Aut(A)$. Let $A^H = \{a \in A : \forall g \in H\ g(a) = a\}$. Prove in detail that $f(A^H) = A^{H^f}$, where $H^f = fHf^{-1}$ is the conjugate of H by f.

[3]Hint: wlog $L \supset R$ is Galois. Consider Sylov 2-subgroup $H < G(L/\mathbb{R})$ and extension $L^H \supset \mathbb{R}$.

[4]Hint: if not, there exists a Galois extension $L \supset \mathbb{C}$ of degree 2^n. $G(L/\mathbb{C})$ jest nilpotent (as a 2-group), hence it contains a subgroup H of index 2. Consider L^H.

[5]Hint: prove that every finite Abelian group is a homomorphic image of some group Z_n^*. Use (without proof) the theorem of Dedekind saying that every arithmetic sequence contains infinitely many primes.