Homework 5
due on Tuesday, May 7

Solve the following problems.

Problem 1. Let $f(x)$ be a monic polynomial of degree n with integer coefficients. Let $x_1, \dots, x_n$ be the roots of f (in the field of complex numbers), so $f = (x - x_1) \dots (x - x_n)$.

a) Prove that for every integer $k > 0$ the polynomial $g_k(x) = (x - x_1^k)(x - x_2^k) \dots (x - x_n^k)$ has integer coefficients.

b) Suppose that $|x_i| \leq 1$ for $i = 1, 2, \dots, n$. Prove that the sequence $g_1, g_2, \dots$ contains only a finte number of different polynomials. Conclude that each x_i is a root of unity.

Problem 2. Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K) = \{\tau_1, \dots, \tau_m\}$. A **normal basis** of L/K is a basis of the form $\tau_1(a), \dots, \tau_m(a)$ for some $a \in L$. We also say that a generates a normal basis of L/K.

a) The action of G on L makes L into a KG-module, where KG is the group ring of G with coefficients in K (review all these concepts if necessary). Prove that L/K has a normal basis if and only if L is free as a KG-module.

b) Suppose that a generates a normal basis of L/K. If M is an intermediate subfield of L/K then let $a_M = \mathrm{Tr}_{L/M}(a)$. Prove that $M = K[a_M]$. Prove that if M/K is normal then a_M generates a normal basis of M/K.

c) Let L_1/K, L_2/K be normal subextensions of L/K such that $L_1 \cap L_2 = K$. Suppose that a_i generates a normal basis of L_i/K, $i = 1, 2$. Prove that $a_1 a_2$ generates a normal basis of $L_1 L_2/K$.

Problem 3. Let L/K be a finite extension of finite fields. Recall that L/K is Galois with cyclic Galois group generated by the automorphism $\phi(x) = x^q$, where $q = |K|$.

a) Prove that the norm $N_{L/K} : L^\times \longrightarrow K^\times$ and trace $T_{L/K} : L \longrightarrow K$ are surjective.

b) Prove that $x^d - 1$ is the minimal polynomial of ϕ considered as an automorphism of the K-vector space L.

c) Consider L as a $K[x]$-module, where $xa = \phi(a)$ for $a \in L$. Using the structure theory of modules over PID prove that L is isomorphic as a $K[x]$-module to $K[x]/(x^d - 1)$. Conclude that L/K has a normal basis.

Problem 4. This problem is about selvability in real radicals. $\mathbb{R}$ denotes the field of real numbers and $\sqrt[n]{a}$ denotes the real n-th root of a (positive when n is even).

a) Suppose $K \subsetneq K(\sqrt[p]{a}) \subseteq \mathbb{R}$, where $a \in K$ and p is a prime. Prove that if $K(\sqrt[p]{a})/K$ is Galois then $p = 2$.

b) Suppose $K \subsetneq K(\sqrt[n]{a}) \subseteq \mathbb{R}$, where $a \in K$ and $n > 1$ is integer. Prove that if $K(\sqrt[n]{a})/K$ is Galois then $[K(\sqrt[n]{a}) : K] = 2$.

c) Suppose $K \subsetneq K(\sqrt[p]{a}) \subseteq \mathbb{R}$, where $a \in K$ and p is a prime. Prove that $[K(\sqrt[p]{a}) : K] = p$.

d) Suppose $K \subseteq M \subseteq K(\sqrt[n]{a}) \subseteq \mathbb{R}$, where $a \in K$ and $n > 1$ is integer. Suppose furthermore that M/K is Galois. Prove that if $n = mp$ for an odd prime p then $M \subseteq K(\sqrt[m]{a})$.

e) Suppose $K \subseteq M \subseteq K(\sqrt[n]{a}) \subseteq \mathbb{R}$, where $a \in K$ and $n = 2^k$ is power of 2. Suppose furthermore that M/K is Galois. Prove that $[M : K] = 2$ and $M = K(\sqrt[d]{a})$ for some d of the form $d = 2^l$. (Hint: Induction on k should work).

f) Suppose that $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_s \subseteq \mathbb{R}$, where $K_i = K_{i-1}(\sqrt[m_i]{a_i})$ for some $a_i \in K_{i-1}$. Prove that if $K \subseteq M \subseteq K_s$ and M/K is Galois then $[M : K] = 2^t$ for some integer $t \leq s$. (Hint: Induction on s should work).

g) Let K be a field, $f \in K[x]$ a separable irreducible polynomial, L/K a splitting field of f and $a \in L$ a root of f. Prove that if $p|[L : K]$ is a prime then there is a subfield $K \subseteq M \subseteq L$ such that $[L : M] = p$ and $L = M(a)$.

h) Let K be a subfield of $\mathbb{R}$. We say that $a \in \mathbb{R}$ is solvable over K by real radicals if there is a chain $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_s \subseteq \mathbb{R}$, where $K_i = K_{i-1}(\sqrt[m_i]{a_i})$ for some $a_i \in K_{i-1}$ and $a \in K_s$. Suppose that all roots of the minimal polynomial $f(x)$ of a over K are real. Prove that if a is solvable over K by real radicals then the Galois group of f is a 2-group.

i) Prove that if $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree 3 with positive discriminant then no root of f is solvable by real radicals.

Problem 5. Let L/K be a finite Galois extension, $\mathrm{Gal}(L/K) = \{\tau_1, \ldots, \tau_m\}$.

a) For $a \in L$, let $a_{i,j} = \tau_i(\tau_j(a))$. Prove that a generates a normal basis of L/K if and only if the matrix $(a_{i,j})$ has a non-zero determinant. **Hint.** We considered a similar result when we proved that the trace form is non-degenerate.

b) Note that $\tau_i\tau_j = \tau_{s(i,j)}$ for some $s(i,j) \in \{1, 2, \ldots, m\}$. Let $H(X_1, \ldots, X_m)$ be the determinant of the matrix $(x_{i,j})$, where $x_{i,j} = X_{s(i,j)}$. Prove that $H \neq 0$ and that a generates a normal basis of L/K if and only if $H(\tau_1(a), \ldots, \tau_m(a)) \neq 0$.

c) Suppose that K is infinite. Prove that if $T(X_1, \ldots, X_m) \in L[X_1, \ldots, X_m]$ is such that $T(a_1, \ldots, a_m) = 0$ for any $a_1, ..., a_m \in K$ then $T = 0$. Chose a basis $u_1, \ldots u_m$ of L over K. Suppose that $H(X_1, \ldots, X_m) \in L[X_1, \ldots, X_m]$ is such that $H(\tau_1(a), \ldots, \tau_m(a)) = 0$ for all $a \in L$. Let $Y_i = \sum_{j=1}^m \tau_i(u_j)X_j$. Consider the polynomial $T(X_1, \ldots, X_m) = H(Y_1, \ldots, Y_m)$. Prove that $T = 0$. Prove that there are $c_{i,j} \in L$ such that $X_i = \sum_{j=1}^m c_{i,j}Y_j$. Conclude that $H = 0$.

d) Prove that if L is infinite then L/K has a normal basis (an earlier exercise asked to prove the same for L finite).