Homework 4

due on Friday, May ??

Solve the following problems.

Problem 1. Recall that we proved the following theorem.

Linear Independence of Characters. Let F be a field, let G be a group, and let $f_1, \ldots, f_m$ be distinct homomorphisms from G to the multiplicative group $F^\times$ of F. Then $f_1, \ldots, f_m$ are linearly independent as functions from G to F.

Consider now a field F, an abelian group A, and homomorphisms $f_1, \ldots, f_m$ from A to the additive group F. We say that $f_1, \ldots, f_m$ are **algebraically dependent** if there is a non-zero polynomial $H \in F[X_1, \ldots, X_m]$ such that $H(f_1(a), \ldots, f_m(a)) = 0$ for all $a \in A$. Suppose that $f_1, \ldots, f_m$ are algebraically dependent and let H be a non-zero polynomial of lowest possible degree such that $H(f_1(a), \ldots, f_m(a)) = 0$ for all $a \in A$.

a) Consider the polynomial $G(X_1, \ldots, X_m, Y_1, \ldots, Y_m) = H(X_1+Y_1, \ldots, X_m+Y_m) - H(X_1, \ldots, X_m) - H(Y_1, \ldots, Y_m)$ as a polynomial in $X_1, \ldots X_m$ with coefficients in $F[Y_1, \ldots, Y_m]$. Prove that $\deg G < \deg H$ and that each coefficient of G (which is a polynomial in $Y_1, \ldots, Y_m$) has degree smaller than $\deg H$. **Hint.** Prove this for any $H \in F[X_1, \ldots, X_m]$ by reducing to the case when F is a monomial.

b) Assume that $G \neq 0$. Prove that there is $b \in A$ such that $G(X_1, \ldots, X_m, f_1(b), \ldots, f_m(b)) \neq 0$. Note that $G(f_1(a), \ldots, f_m(a), f_1(b), \ldots, f_m(b)) = 0$ for all $a \in A$ and derive a contradiction. This proves that $G = 0$. Polynomials H for which $G = 0$ are called **additive** polynomials.

c) Let H be an additive polynomial. Let $h_i(X) = H(0, \ldots, X, \ldots, 0)$, i.e. we set $X_i = X$ and $X_j = 0$ for $j \neq i$. Prove that each h_i is an additive polynomial in one variable and $H(X_1, \ldots, X_m) = h_1(X_1) + \ldots + h_m(X_m)$.

d) Let $h(X)$ be an additive polynomial in one variable. Let p be the characteristic of F. Prove that $h(X) = cX$ for some $c \in F$ if $p = 0$ and $h(X) = \sum_{i=0}^{t} c_i X^{p^i}$ for some $c_i \in F$ if $p > 0$.

e) Suppose now that A is a field and $f_1, \ldots, f_m$ are distinct embeddings of A into F which are algebraically dependent. Prove that the characteristic p of F is positive and there are indices i, j such that $f_i = f_j^{p^k}$ for some k. Conclude that if K is an infinite field and G is a finite group of automorphisms of K then the elements of G are algebraically independent.

f) This part outlines a different proof of the last part of e). Let $L = K^G$ be the fixed field of G, $G = \{f_1, \ldots, f_m\}$. Prove that if $T(X_1, \ldots, X_m) \in K[X_1, \ldots, X_m]$ is such that $T(a_1, \ldots, a_m) = 0$ for any $a_1, ..., a_m \in L$ then $T = 0$. Chose a basis $u_1, \ldots u_m$ of K over L. Suppose that $H(f_1(a), \ldots, f_m(a)) = 0$ for all $a \in K$. Let $Y_i = \sum_{j=1}^{m} f_i(u_j) X_j$. Consider the polynomial $T(X_1, \ldots, X_m) = H(Y_1, \ldots, Y_m)$. Prove that $T = 0$. Prove that there are $c_{i,j} \in K$ such that $X_i = \sum_{j=1}^{m} c_{i,j} Y_j$. Conclude that $H = 0$.

Problem 2. Let L/K be a finite Galois extension, $\mathrm{Gal}(L/K) = \{f_1, \ldots, f_m\}$. A **normal basis** of L/K is a basis of the form $f_1(a), \ldots, f_m(a)$ for some $a \in L$. We also say that a generates a normal basis of L/K.

a) Let $a_{i,j} = f_i(f_j(a))$. Prove that $f_1(a), \ldots, f_m(a)$ is a normal basis of L/K if and only if the matrix $(a_{i,j})$ has a non-zero determinant. **Hint.** We did a similar result when we proved that the trace form is non-degenerate.

b) Note that $f_i f_j = f_{s(i,j)}$ 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 $f_1(a), \ldots, f_m(a)$ is a normal basis of L/K if and only if $H(f_1(a), \ldots, f_m(a)) \neq 0$.

c) Prove that if L is infinite then L/K has a normal basis (in the next exercise you will prove the same for L finite).

d) Prove that L/K has a normal basis if and only if L is free as a KG-module.

e) Let $f_1(a), \ldots, f_m(a)$ be a normal basis for 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 for L/K.

f) 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 for L_i/K, $i = 1, 2$. Prove that $a_1 a_2$ generates a normal basis for $L_1 L_2/K$.

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. a) Let p be a prime and let K be a field of characteristic not equal to p which contains primitive p-th root of 1 and, if $p = 2$, also a primitive 4-th root of 1. Fix $a \in K$. In a fixed algebraic closure of K, we choose elements u_n such that $u_0 = a$ and $u_{n+1}^p = u_n$ for all n. Let $K_0 = K$ and $K_{n+1} = K_n[u_n]$. Prove that if $K_n \neq K_{n-1}$ then $K_n \subsetneq K_{n+1}$. **Hint.** Note that K_n/K_{n-1} is cyclic of degree p. Assuming $K_n = K_{n+1}$ look at the norm map from K_n to K_{n-1} or analyze the action of the Galois group to get a contradiction.

b) Let p be the characteristic of a field K and let $a \in K$. Suppose that $x^p - x - a$ is irreducible over K and let u be a root of $x^p - x - a$. Prove that the trace map T from $K[u]$ to K is surjective. Let $w \in K[u]$ be such that $T(w) = a$. Prove that $x^p - x - w$ is irreducible over $K[u]$.

c) Let p be the characteristic of a field K and let $a \in K$. Suppose that $x^p - a$ is irreducible over K. Prove that $x^{p^n} - a$ is irreducible over K for all n.

d) Let L be an algebraically closed field and let K be a subfield of L such that L/K is finite. Prove that L/K is separable (use c)). Conclude that L/K is Galois. Note that if p is a prime and $p|[L : K]$ then there is an intermediate subfield M of L/K such L/M is cyclic of degree p. Use b) to prove that p is not equal to the characteristic of L. Use a) to prove that $p = 2$ and primitive 4-th root of 1 is not in M. Thus $\mathrm{Gal}(L/K)$ is a 2-group. Let i be a primitive 4-th root of 1. Note that no non-trivial element of $\mathrm{Gal}(L/K)$ can fix i. Conclude that G has order 2 and $L = K(i)$.

e) Let L be an algebraically closed field and let K be a subfield of L such that L/K is finite.

We have proved that $[L : K] = 2$ and $L = K[i]$, with $i^2 = -1$. Prove that for any non-zero $a \in K$ either a or $-a$ is a square in K but not both. Prove that the set of squares in K is closed under addition. For $a, b \in K$ define $a < b$ if $b - a$ is a square in K. Prove that $<$ is a linear order on K. Conclude that K has characteristic 0. Fields K such that the algebraic closure of K has degree 2 over K are called **real closed**.

Problem 5. Consider the polynomial $p(x) = x^4 + 5x^2 + 12x + 13$.

a) Prove that p is irreducible over $\mathbb{Q}$. Compute the discriminant of p.

b) Let x_1, x_2, x_3, x_4 be the roots of p. Let $z_1 = x_1x_2 + x_3x_4$, $z_2 = x_1x_3 + x_2x_4$ and $z_3 = x_1x_4 + x_2x_3$. Let $q(x) = (x - z_1)(x - z_2)(x_- z_3)$. Explain why q should have rational coefficients and compute these coefficients. Then find the roots of q.

c) Consider the Galois group G of p as a subgroup of S_4 via its permutation action on the roots of p. Prove that $\mathbb{Q}(x_1, x_2, x_3, x_4)/Q(z_1, z_2, z_3)$ is Galois with Galois group $G \cap V$, where V is the unique normal subgroup of S_4 of order 4. Conclude that the Galois group of p is contained in a Sylow 2-subgroup of S_4. Prove that $V \subseteq G$ and conclude that G is isomorphic to the dihedral group of order 8 (one way to do that is to show that $Q(x_1, x_2, x_3, x_4)$ contains two quadratic extensions of $\mathbb{Q}$).

c) Express the roots of p in radicals.