Solutions to the Midterm

Problem 1. Let L/K be a finite extension of fields, let M be the separable closure of K in L and let $\phi : K \longrightarrow F$ be an embedding of K into an algebraically closed field F. Prove that ϕ can be extended to exactly $[M : K]$ embeddings of L into F.

Solution: Since M/K is separable, ϕ extends to exactly $[M : K]$ embeddings of M into F. Let ψ be any such extension. We know that it can be extended in at least one way to an embedding of L into F. So it suffices to show that there is exactly one such extension. In fact, since L/M is purely inseparable, for every $a \in L$ there is a natural number m such that $a^{p^m} \in M$, where p is the characteristic of K. If η_1, η_2 are two extensions of ψ to L then

$$\eta_1(a)^{p^m} = \eta_1(a^{p^m}) = \psi(a^{p^m}) = \eta_2(a^{p^m}) = \eta_2(a)^{p^m}.$$

Since raising to p^m-th power is injective on fields of characteristic p, we see that $\eta_1(a) = \eta_2(a)$. It follows that $\eta_1 = \eta_2$.

Problem 2. Let L/K be an algebraic extension (not necessarily finite). Prove that any homomorphism $\phi : L \longrightarrow L$ which is identity on K is an automorphism.

Solution: Since any homomorphism of fields is injective, we only need to show that ϕ is surjective. Let $a \in L$ and let $p(x) \in K[x]$ be the minimal polynomial of a over K. Note that for any root u of p in L the image $\phi(u)$ is again a root of p in L. Thus ϕ maps the set S of roots of p in L to itself. Since S is finite and ϕ is injective, ϕ is a bijection on S. In particular $a = \psi(b)$ for some $b \in S$. This proves that ϕ is surjective, hence it is an isomorphism.

Problem 3. Let p be a prime and let L be the splitting field of $x^p - 1$ over $\mathbb{Q}$. Thus $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic of order $p - 1$. Let ξ be a primitive p-th root of unity in L. For a subgroup H of $\mathrm{Gal}(L/\mathbb{Q})$ define $a_H = \sum_{\sigma \in H} \sigma(\xi)$.

1. Prove that $L^H = \mathbb{Q}(a_H)$.
2. For $p = 7$, find the minimal polynomial of a_H for every subgroup H of $\mathrm{Gal}(L/\mathbb{Q})$.

Solution: Since $L = \mathbb{Q}(\xi)$ and $[L : \mathbb{Q}] = p - 1$, the elements $1, \xi, \xi^2, ..., \xi^{p-2}$ form a basis of L over $\mathbb{Q}$. It follows $\xi, \xi^2, ..., \xi p - 1$ is also a basis of L over $\mathbb{Q}$. Note now that the sets $\{\xi, \xi^2, ..., \xi p - 1\}$ and $\{\sigma(\xi) : \sigma \in \mathrm{Gal}(L/\mathbb{Q})$ coincide. Thus the latter set is a basis of L over $\mathbb{Q}$. Given $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, we have

$$\tau(a_H) = \sum_{\sigma \in H} (\tau\sigma)(\xi) = \sum_{\sigma \in \tau H} \sigma(\xi).$$

From the linear independence of $\{\sigma(\xi) : \sigma \in \mathrm{Gal}(L/\mathbb{Q})$ we see now that $a_H = \tau(a_H)$ iff $H = \tau H$, which in turn is equivalent to $\tau \in H$. Clearly this implies 1.

For 2. note that the cyclic group of order 6 has four subgroups, namely cyclic groups of orders $1, 2, 3, 6$. If H has order 1 then $a_H = \xi$ has minimal polynomial $\Phi_7 = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$. If H has order 6 then $a_H = \xi + \xi^2 + ... + \xi 6 = -1$, so its minimal polynomial is $x + 1$.

Recall now that $\mathrm{Gal}(L/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/7\mathbb{Z}7)^\times$, where the class of an integer i in $(\mathbb{Z}/7\mathbb{Z}7)^\times$ corresponds to the automorphism σ_i which maps ξ to ξ^i. The subgroup of order 3 of $\mathrm{Gal}(L/\mathbb{Q})$ is then generated by σ_2 and the subgroup of order 2 is generated by σ_{-1}. It follows that $a_H = \xi + \xi^2 + \xi^4$ if $|H| = 3$ and $a_H = \xi + \xi^{-1}$ if $|H| = 2$.

Suppose first that $|H| = 3$. By 1., a_H is of degree 2 over $\mathbb{Q}$. The orbit of a_H under the action of $\mathrm{Gal}(L/\mathbb{Q})$ consists of two elements, namely a_H and $b_H = \sigma_{-1}(a_H) = \xi^3 + \xi^5 + \xi^6$. Thus the minimal polynomial of a_H is $(x - a_H)(x - b_H) = x^2 - (a_H + b_H)x + a_H b_H$. Clearly $a_H + b_H = -1$ and it is easy to compute that $a_H b_H = 2$. We see that $x^2 + x + 2$ is the minimal polynomial of a_H and $L^H = \mathbb{Q}(\sqrt{-7})$.

Finally, if $|H| = 2$, then the conjugates of $a_H = \xi + \xi^6$ are $b_H = \xi^3 + \xi^4$ and $c_H = \xi^2 + \xi^5$. Thus

$$(x - a_H)(x - b_h)(x - c_H) = x^3 - (a_H + b_H + c_H)x^2 + (a_H b_H + a_H c_H + b_H c_H)x - a_H b_H c_H$$

is the minimal polynomial of a_H. Now $a_H + b_H + c_H = -1$, $a_H b_H + a_H c_H + b_H c_H = -2$ and $a_H b_H c_H = 1$. Thus the minimal polynomial of a_H is $x^3 + x^2 - 2x - 1$.

Problem 4. Let K be a field of characteristic different from 2.

1. Let $a, b \in K$ be such that none of a, b, ab is a square in K. Prove that $K(\sqrt{a}, \sqrt{b})$ is a Galois extension of K with Galois group isomorphic to the Klein 4-group (i.e. the product of two copies of the cyclic group of order 2).

2. Suppose that L/K is a Galois extension with the Galois group isomorphic to the Klein 4-group. Show that $L = K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K$ such that none of a, b, ab is a square in K.

Solution: 1. Note that $L = K(\sqrt{a}, \sqrt{b})$ is a splitting field of the polynomial $(x^2 - a)(x^2 - b)$, which is separable (if the characteristic of K is not 2). Thus L/K is Galois. We claim that the subfields $L_1 = K(\sqrt{a})$, $L_2 = K(sqrtb$ are different. In fact, note that every automorphism of L/K is either trivial on L_1 or maps $\sqrt{a}$ to $-\sqrt{a}$ and similar claim holds for L_2. Thus, if $L_1 = L_2$, then every automorphism of L either fixes both $\sqrt{a}$, $\sqrt{b}$ or maps each of them to its negative. It follows that every automorphism of L fixes $\sqrt{a}\sqrt{b}$. Thus $\sqrt{a}\sqrt{b} \in K$, which implies that ab is a square in K, a contradiction. We see then that $L_1 \neq L_2$. Clearly $[L_1 : K] = [L_2 : K] = 2$, $L = L_1 L_2$ and $L_1 \cap L_2 = K$. From a general result proved in class, we see that $\mathrm{Gal}L/K$ is isomorphic to the product $\mathrm{Gal}L_1/K \times \mathrm{Gal}L - 2/K$, which is the Klein 4-group. (Alternatively, observe that $[L : K] = 4$. Thus $\mathrm{Gal}L/K$ has order 4 and has at least 2 subgroups of order 2, corresponding to L_1 and L_2. Since the Klein 4=group is the only group of order 4 with more that one subgroup of order 2, the result follows).

2. Note that the Klein 4-group has three distinct subgroups of order 2. Thus L/K has three distinct subfields of degree 2 over K. Consider two of this subfields L_1 and L_2. Both fields are Galois over K. Let σ_i be an automorphism of L/K which is non-trivial on L_i, $i = 1, 2$. Thus $\mathrm{Gal}(L_i/K) = \{\mathrm{id}, \sigma_i\}$. There is $a_i \in L_i$ such that $\sigma_i(a_i) \neq a_i$. Let $x_i = \sigma_i(a_i) - a_i \neq 0$. Thus $\sigma_i(x_i) = \sigma_i^2(a_i) - \sigma_i(a_i) = -x_i$. It follows that $x_i \notin K$. On the other hand, $\sigma_1(x_i^2) = (-x_i)^2 = x_i^2$, so $x_i^2 \in K$. In other words, $L_1 = K(\sqrt{a})$, $L_2 = K(\sqrt{b})$, where $a = x_1^2$ and $b = x_2^2$. Clearly neither a nor b is a square in K (since $L_i \neq K$) and ab is not a square in K since $L_1 \neq L_2$. Thus $L = L_1 L_2 = K(\sqrt{a}, \sqrt{b})$.

****

The following problem is optional. You may earn extra credit, but concentrate first on problems 1-4.

Problem 5. Let K be a filed. Suppose that L is an algebraic extension of K such that every polynomial in $K[x]$ has a root in L and let F be an algebraically closed

field containing L.

1. Show that every finite separable extension M/K contained in F is contained in L. Hint: Consider the normal closure of M inside F and note that it is a simple extension of K. Conclude that if $\mathrm{char}K = 0$ then L is algebraically closed.

2. Show that if $p = \mathrm{char}K$ is a prime then for any $b \in F$ algebraic over L we have $b^{p^k} \in L$ for some k.

3. Show that if $p = \mathrm{char}K$ is a prime then $a^{1/p^m} \in L$ for every $a \in K$ and every m. Conclude that if $f \in K[x]$ is separable then there is a separable polynomial $f_m \in L[x]$ such that $f_m(x)^{p^m} = f(x^{p^m})$ for every natural number m.

4. Use 2 and 3 to show that every element of F algebraic over L is separable over L. Conclude that L is algebraically closed.

Solution: Let us first note that the algebraic closure of K in F (i.e. the set of all elements of F which are algebraic over K) is algebraically closed and contains L. Thus we may (and will) assume that F is an algebraic closure of K, i.e. that all elements of F are algebraic over K. The problem establishes then that $F = L$.

If M is a finite and separable extension of K then the normal closure N of M in F is a finite, normal and separable extension of K. Thus $N = K(u)$ for some u. Let f be the minimal polynomial of u over K. Since N/K is normal and f has a root in N (namely u), we see that all roots of f are in N and $N = K(w)$ for any root w of f. But one such w belongs to L so $N = K(w) \subseteq L$. It follows that every element of F separable over K belongs to L. If $\mathrm{char}K = 0$ then all elements are separable, hence $L = F$. This proves 1.

Suppose now that $p = \mathrm{char}K$ is positive. Then from 1. we know that L contains all elements of F separable over K. If $b \in F$ then we know that b^{p^k} is separable over K for some k. Thus $b^{p^k} \in L$ for some k. This establishes 2.

Let $a \in K$. Consider the polynomial $x^{p^m} - a \in K[x]$. It has a root b in L. Thus $a^{1/p^m} \in L$. For the last conclusion of 3. it suffices to consider an irreducible separable polynomial $f(x) = f_0 + f_1 x + ... + f_t x^t \in K[x]$. Let $f_m(x) = f_0^{1/p^m} + f_1^{1/p^m} x +$

$... + f_t^{1/p^m} x^t$. It follows from what we have just proved that $f_m \in L[x]$. Clearly $f_m(x)^{p^m} = f(x^{p^m})$. We just need to see that f_m is separable. Consider the embedding $L \longrightarrow L$ which sends a to a^{p^m}. It defines an embedding $L[x] \longrightarrow L[x]$ which takes f_m to f. This embedding takes f'_m to f' and $(gcd)(f'_m, fm)$ to $(gcd)(f', f)$. Since $(gcd)(f', f) = 1$, we see that $(gcd)(f'_m, fm) = 1$ and therefore f_m has no multiple roots, hence is separable.

Suppose now that $b \in F$. Then, as in the solution to 2., b^{p^m} is separable over K for some k, hence $b^{p^m} \in L$. Let f be the minimal polynomial of b^{p^m} over K, so f is separable. The polynomial f_m from 3. has coefficients in L, is separable over L and $f_m(b)^{p^m} = f(b^{p^m}) = 0$, i.e $f_m(b) = 0$. Thus b is a root of a separable polynomial over L, i.e. b is separable over L. On the other hand, the minimal polynomial of b over L divides $x^{p^m} - b^{p^m} \in L[x]$. Since this polynomial has only one root (namely b), any factor of this polynomial over L, which is both separable and irreducible over L must be linear. Thus the minimal polynomial of b over L is linear, i.e. $b \in L$. This proves that $L = F$.