Math 603, Spring 2003, HW 6, due 4/21/2003

Part A

AI) If k is a field and $f \in k[T]$, suppose f has degree n and has n distinct roots $\alpha_1, \ldots, \alpha_n$ in some extension of k. Write $\Omega = k(\alpha_1, \ldots, \alpha_n)$ for the splitting field of f and further take $n+1$ independent indeterminates $X, u_1, \ldots, u_n$ over Ω. Let $\widetilde{k} = k(u_1, \ldots, u_n)$, write $\widetilde{\Omega}$ for $\widetilde{k}(\alpha_1, \ldots, \alpha_n)$ and let $\omega = \alpha_1 u_1 + \cdots + \alpha_n u_n \in \widetilde{\Omega}$. If σ is an *arbitrary permutation* of $\alpha_1, \ldots, \alpha_n$ set

$$\sigma\omega = \sigma(\alpha_1)u_1 + \cdots + \sigma(\alpha_n)u_n,$$

and finally set

$$h(X) = \prod_{\sigma \in \mathcal{S}_n} (X - \sigma\omega).$$

(a) Show that $h(X)$ has coefficients in $k[u_1, \ldots, u_n]$.

(b) Split $h(X)$ into irreducible factors in $\widetilde{k}[X]$; show all the factors have the same degree, r. (Hint: natural irrationalities). Moreover, prove if $\sigma\omega$ is a root of a given factor, the other roots of this factor are exactly the $\tau \circ \omega$, with $\tau \in \mathfrak{g}(\Omega/k)$. Hence, prove that $r = \#\big(\mathfrak{g}(\Omega/k)\big)$.

(c) Using (b), give a procedure for explicitly determining those permutations, $\sigma \in \mathcal{S}_n$, which belong to $\mathfrak{g}(\Omega/k)$. Illustrate your procedure with the examples: $k = \mathbb{Q}$, $f = T^3 - 2$ and $f = T^4 + T^3 + T^2 + T + 1$.

AII) Here k is a field and Ω is a finite normal extension of k. Prove that there exists a normal tower of fields

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n = \Omega$$

so that

i) the first r of these extensions are separable and the set $\{\mathfrak{g}(k_i/k_{i-1}) \mid 1 \leq i \leq r\}$ is exactly the set of composition factors of $\mathfrak{g}(\Omega/k)$, and

ii) The last $n-r$ are each purely inseparable over the previous and k_j arises from k_{j-1} by adjunction of a root of $X^p - a_j$, with $a_j \in k_{j-1}$. (Here, $p = \mathrm{char}(k)$.)

AIII) Let $g_1, \ldots, g_n$ be polynomials (one variable) with coefficients in $k = k_0, \ldots, k_{n-1}$ respectively, and with k_j the splitting field for g_j. In this case, we say k_n *arises from the successive solution of a chain of equations* $g_1 = 0, g_2 = 0, \ldots, g_n = 0$. If f is a polynomial, we say $f = 0$ *can be solved by means of an auxiliary chain,* $g_i = 0$, *of equations* $\iff$ k_n contains a splitting field for f. When the $g_i(X)$ have the special form $g_i(X) = X^{m_i} - a_i$, we say $f = 0$ may be solved by radicals.

(a) Suppose $f = 0$ may be solved by means of the auxiliary chain $g_1 = 0, \ldots, g_n = 0$. Let $\gamma(G)$ denote the set of simple constituents (composition factors) of a given finite group, G. Prove that $\gamma\big(\mathfrak{g}_k(f)\big) \subseteq \bigcup \gamma\big(\mathfrak{g}_{k_{j-1}}(g_j)\big)$.

(b) Prove "Galois' Theorem": if k is a field, $f \in k[X]$, and Ω a splitting field for f over k, assume $\big(\mathrm{char}(k), [\Omega : k]\big) = 1$; then $f = 0$ is solvable by radicals $\iff$ $\mathfrak{g}_k(f)$ is a solvable group.

AIV) Here k is a field, α is a root of an irreducible polynomial, $f \in k[X]$.

(a) Prove: α lies in a field extension, L, of k obtained by successive solution of a chain of *quadratic* equations $g_1 = 0, \ldots, g_n = 0$ $\iff$ the degree of a splitting field for f over k is a power of 2.

(b) Given a line in the plane, we conceive of the line as the real line and the plane as $\mathbb{C}$. *But*, no numbers are represented on the line. However, two points are indicated on the line; we take these as 0 and 1 and label them so. We are given a straight edge (NO MARKINGS ON IT) and a pair of dividers (no scale on it either) which we can set to any length and which will hold that length. But, if we reset the dividers, the original setting cannot be recaptured if not marked on our plane as a pair of points "already constructed". We can use our implements to make any finite number of the following moves:

i. Set the dividers to a position corresponding to two points already constructed, make any arc or circle with the dividers where one leg is at a point already constructed. (A point is constructed iff it is the intersection of an arc and a line, an arc and an arc, a line and a line.)

ii. Given any pair of previously constructed points use the straight edge to draw a line or segment of a line through these points.

You should be able to see that from 0 and 1 we can construct $p/q \in \mathbb{Q}$ (all p, q) therefore it is legitimate to label $\mathbb{Q}$ on our real axis. Call a point $(x, y) \in \mathbb{C}$ constructible iff its real and imaginary parts are constructible; that is these numbers, constructed as lengths, can be obtained from $\mathbb{Q}$ by successive solution of a chain of quadratic equations.

(c) Prove

i. The duplication of a cube by straight edge and dividers is impossible

ii. The trisection of an angle by straight edge and dividers is impossible (try $\pi/3$).

AV) What is wrong with the following argument?
Let k be a field, write $f(X) \in k[X]$, $\deg(f) = n$, and suppose f has n distinct roots $\alpha_1, \ldots, \alpha_n$, in a suitable extension field L/k. Write Ω for the normal extension $k(\alpha_1, \ldots, \alpha_n)$. An element, ω, of Ω has the form $\omega = g(\alpha_1, \ldots, \alpha_n)$, where g is a polynomial in n variables with coefficients in k. Let σ be an arbitrary permutation of the α_i, then σ maps $g(\alpha_1, \ldots, \alpha_n)$ to $g(\alpha'_1, \ldots, \alpha'_n)$ where $\alpha'_j = \sigma(\alpha_j)$. If $h(\alpha_1, \ldots, \alpha_n)$ is another polynomial with coefficients in k, then $h(\alpha_1, \ldots, \alpha_n) \mapsto h(\alpha'_1, \ldots, \alpha'_n)$ by σ and we have

$$g(\alpha_1, \ldots, \alpha_n) + h(\alpha_1, \ldots, \alpha_n) \to g(\alpha'_1, \ldots, \alpha'_n) + h(\alpha'_1, \ldots, \alpha'_n)$$
$$g(\alpha_1, \ldots, \alpha_n)h(\alpha_1, \ldots, \alpha_n) \to g(\alpha'_1, \ldots, \alpha'_n)h(\alpha'_1, \ldots, \alpha'_n).$$

Thus, we have an automorphism of Ω and the elements of k remain fixed. So, the arbitrary permutation, σ, belongs to the group of k-automorphisms of Ω; hence, the latter group has order greater than or equal to $n!$. By Artin's Theorem, $[\Omega : k] \geq n!$.

AVI) If k is a field, $f \in k[X]$ a separable polynomial and Ω is a splitting field for f over k, write $\mathfrak{g} = \mathfrak{g}(\Omega/k)$ and consider $\mathfrak{g}$ as a subgroup of the permutation group on the roots of f. Show that $\mathfrak{g}$ is a transitive permutation group $\iff$ f is an irreducible polynomial over k. Use this to give a necessary condition that $\sigma \in \mathcal{S}_n$ actually belongs to $\mathfrak{g}_k(f)$, for f an arbitrary separable polynomial of degree n over k. Illustrate your condition by finding the Galois groups over $\mathbb{Q}$ of the polynomials: $X^5 - 1$, $X^5 + X + 1$.

AVII) Here, K is a finite field of q elements and q is odd.

(a) Let $\mathrm{sq} : K^* \to K^*$ be the homomorphism given by $\mathrm{sq}(x) = x^2$. Show that $\#\ker \mathrm{sq} = \#\operatorname{coker} \mathrm{sq} = 2$ and $\#\operatorname{Im} \mathrm{sq} = (q-1)/2$.

(b) Prove:

$$(\forall x \in K^*)\left(x^{(q-1)/2} = \begin{cases} 1 & \text{if } x \text{ is a square in } K \\ -1 & \text{otherwise} \end{cases}\right)$$

(c) If $K = \mathbb{F}_p$, then K contains a square root of -1 iff $p \equiv 1 \bmod 4$.

(d) For any finite field, K, every element of K is a sum of squares.

AVIII) If k is a field of characteristic zero and $f \in k[X]$ is a monic polynomial, factor f into monic irreducible polynomials in $k[X]$ and set

$$f = g_1 g_2^2 \cdots g_r^r$$

where g_j is the product of the distinct irreducible factors of f which divide f with exact exponent j. Prove that the g.c.d. of f and its derivative f', is

$$g_2 g_3^2 \cdots g_r^{r-1}.$$

Assume Euclid's algorithm for finding the g.c.d. of two polynomials. Show that $g_1, \ldots, g_r$ may be determined constructively. If n is an integer, illustrate with

$$f(X) = X^n - 1 \in \mathbb{Q}[X].$$

AIX) If k is a field and f, g are non-constructible polynomials in $k[X]$, with f irreducible, prove that the degree of every irreducible factor of $f\big(g(X)\big)$ in $k[X]$ is divisible by $\deg f$.

Part B

BI) If k is a field, X is transcendental over k, and $f(X) \in k[X]$ is irreducible in $k[X]$, write $\alpha_1, \ldots, \alpha_n$ for a full set of roots of f in a suitable extension field of k. If $\mathrm{char}(k) = 0$, prove that none of the differences $\alpha_i - \alpha_j$ $(i \neq j)$ can lie in k. Give a counterexample for $\mathrm{char}(k) = p > 0$ (*any* prime p, i.e. $(\forall p)$).

BII) Let $k \subseteq K$ be two fields of characteristic zero. Assume the following two statements:

i. Every $f(X) \in k[X]$ of *odd* degree has a root in K

ii. $(\forall \alpha \in K)(X^2 - \alpha$ has a root in $K)$

(a) Prove: each non-constant polynomial $g \in k[X]$ has a root in K.

(b) Assume as well that K/k is normal of finite degree. Prove the K is algebraically closed. (Suggestion: use induction on ν where $\deg g = 2^\nu n_0$ (n_0 odd). If $r \in \mathbb{Z}$, set $\gamma_{ij}^{(r)} = \alpha_i + \alpha_j + r\alpha_i\alpha_j$, where $\alpha_1, \ldots, \alpha_n$ are the roots of g in some $\Omega \supseteq K$. Fix r, show $\exists$ a polynomial $h(X) \in k[X]$, and the $\gamma_{ij}^{(r)}$ are roots of h; all i, j. Show some $\gamma_{ij}^{(r)} \in K$; now vary r and find $r_1 \neq r_2$ so that $\gamma_{ij}^{(r_1)} \in K$, $\gamma_{ij}^{(r_2)} \in K$.)

(c) Take $k = \mathbb{R}$, $K = \mathbb{C}$, by elementary analysis, i and ii hold. Deduce $\mathbb{C}$ is algebraically closed (Gauss' first proof).

BIII) Let $\mathbb{Q}$ be the rational numbers, $\mathbb{R}$ the real numbers , X a transcendental over $\mathbb{R}$ and suppose $f \in \mathbb{Q}[X]$ is a polynomial of degree 3 irreducible in $\mathbb{Q}[X]$ having three real roots α, β, γ. Show that if

$$k_0 = \mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_m$$

is a finite chain of fields each obtained from the preceding one by adjunction of a *real* radical $\rho_j = \sqrt[n_j]{c_j}$ $(n_j \in \mathbb{Z}, n_j > 0, c_j \in k_{j-1})$, the field k_m *cannot* contain ANY of the roots, α, β, γ of f. (Suggestion: if wrong, show we may assume each n_j is prime, let k_j be the field with maximal j where f is still irreducible. If $\alpha \in k_{j+1}$ show $\rho_{j+1} \in k_j(\alpha)$.) This is the famous "casus irreducibilis" of the cubic equation $f = 0$: if the three roots are real, the equation cannot be solved by real radicals.

BIV) Here, f is an irreducible quartic polynomial with coefficients in k; assume f has four distinct roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in some extension field of k. Write $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $L = k(\beta)$, and let Ω be $k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

(a) Assume $\mathfrak{g}(\Omega/k)$ has full size, i.e., 24, find $\mathfrak{g}(\Omega/L)$.

(b) Show that, in any case, β is the root of a cubic polynomial, k, with coefficients in k (Lagrange's "cubic resolvent" for f).

BV) Let k be a field, $\mathrm{char}(k) \neq 2$, write K/k for an extension of degree 2 and L/K for an extension also of degree 2.

(a) Show $\exists\, \alpha, \beta$ with $\alpha \in K$, in fact $K = k(\alpha)$, and $\alpha^2 = a \in k$ and $\beta \in L$, $\beta^2 = u + v\alpha$; $u, v \in k$ and $L = K(\beta)$. (All this is very easy).

(b) Let Ω be a normal closure of k containing L. Show that $[\Omega : k]$ is 4 or 8. In the case $v = 0$ (part (a)), show $\Omega = k(\alpha, \beta) = L$ and that $\exists\, \sigma, \tau \in \mathfrak{g}(\Omega/k)$ so that $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$, $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. Determine precisely the group $\mathfrak{g}(\Omega/k)$.

(c) When $v \neq 0$, let β_1 be a conjugate, not equal to $\pm\beta$, of β. Prove $\Omega = k(\beta, \beta_1)$ and that $\exists\, \sigma \in \mathfrak{g}(\Omega/k)$ such that $\sigma(\beta) = \beta_1$ and $\sigma(\beta_1)$ is one of β or $-\beta$.

(d) Show if $[\Omega : k] = 8$ we may assume in (c) that σ maps β_1 to $-\beta$. Prove σ is an element of order 4 and that $\exists\, \tau \in \mathfrak{g}(\Omega/k)$, of order 2, with $\tau^{-1}\sigma\tau = \sigma^{-1}$. Deduce that $\mathfrak{g}(\Omega/k) = \mathrm{Gp}\{\sigma, \tau\}$; which of the two non-abelian groups of order 8 is it?

(e) Illustrate (a)-(d) with a discussion of $X^4 - a$ over $\mathbb{Q}$.

(f) With the above notation, show that the normal closure of K in cyclic of degree 4 $\iff$ a can be written as the sum of two squares, $b^2 + c^2$, in k. (Hints: if Ω is the field above, show $\mathfrak{g}(\Omega/k)$ is cyclic, order 4, iff Ω contains exactly one subfield of degree 2 over k. Then $u^2 - av^2$ must equal aw^2 for some $w \in k$. Now show a is the sum of two squares. You may need to prove that -1 is a square $\implies$ every element of k is a sum of two squares in k; c.f. AVII.) Investigate, from the above, which primes, $p \in \mathbb{Z}$, are the sum of two squares in $\mathbb{Z}$.

BVI) (a) Say k is a field, $\mathrm{char}(k) > 2$; let $K = k(X, Y)$ where X and Y are independent transcendentals over k. Write $L = K(\theta)$, where θ is a root of

$$f(Z) = Z^{2p} + XZ^p + Y \in K[Z].$$

Show that L/K is inseparable yet does not contain any purely inseparable elements over K. (Suggestion: first show f is irreducible and say $\exists\, \beta \in L, \beta^p \in K, \beta \notin K$. Then prove f becomes reducible in $K(\beta)[Z]$ and that then $X^{1/p}$ and $Y^{1/p}$ would lie in L. Prove then that $[L : K] \geq p^2$.)

(b) Find the Galois group $\mathfrak{g}(\Omega/K)$ where Ω is a normal closure of L/K.

(c) Now just assume $\mathrm{char}(k) \neq 2$, write $K = k(X)$ in this case. Let σ, τ be the idempotent k-automorphisms of K given by $\sigma(X) = -X, \tau(X) = 1 - X$ (i.e., $\sigma\big(f(X)\big) = f(-X)$, etc.). Show the fixed field of σ is $k(X^2)$, that of τ is $k(X^2 - X)$. If $\mathrm{char}(k) = 0$, show that $\mathrm{Gp}\{\sigma, \tau\}$ is an infinite group and prove that $k = k(X^2) \cap k(X^2 - X)$.

(d) Now assume again $\mathrm{char}(k) = p > 2$. Show in this case $k(X^2) \cap k(X^2 - X)$ is strictly bigger than k—determine it explicitly and find the degree

$$\big[k(X) : (k(X^2) \cap k(X^2 - X))\big].$$

(e) What is the situation in (c) and (d) if $\mathrm{char}(k) = 2$?

BVII) (Various Galois groups). Determine the Galois groups of the following polynomials over the given fields:

(a) $(X^2 - p_1) \cdots (X^2 - p_t)$ over $\mathbb{Q}$, where $p_1, \ldots, p_t$ are distinct prime numbers.

(b) $X^4 - t$ over $\mathbb{R}(t)$.

(c) $X^p - m$ over $\mathbb{Q}$, where p is a prime number and m is a square-factor free integer. (Hint: here, $\mathfrak{g}$ fits into a split exact sequence of groups

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathfrak{g} \xrightarrow{\leftarrow\!\!-} ? \to 0.)$$

(d) $X^8 - 2$ over $\mathbb{Q}(\sqrt{2})$, over $\mathbb{Q}(i)$, over $\mathbb{Q}$. (C.f. BV)

BVIII) (a) Here K/k is a finite extension of fields. Show the following are equivalent:

i. K/k is separable

ii. $K \otimes_k L$ is a product of fields (product in the category of rings) for *any* field L over k

iii. $K \otimes_k \overline{k}$ is a product of fields

iv. $K \otimes_k K$ is a product of fields.

(b) Now assume K/k is also a normal extension, and let

$$K_{\mathrm{pi}} = \{\alpha \in K \mid \alpha \text{ is purely inseparable over } k\}.$$

For the map

$$\theta : K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}} \to K_{\mathrm{pi}} \ \textit{via}\ \theta(\xi \otimes \eta) = \xi\eta,$$

show that the kernel of θ is exactly the nilradical of $K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}} \to K_{\mathrm{pi}}$

(c) Prove: if K/k is a finite normal extension, then $K \otimes_k K$ is an Artin ring with exactly $[K : k]_{\mathrm{s}}$ prime ideals. The residue field of all its localizations at these prime ideals are each the same field, K. A necessary and sufficient condition that K/k be purely inseparable is that $K \otimes_k K$ be a local ring. (Hints: $K = K_{\mathrm{s}} \otimes_k K_{\mathrm{pi}}$ and the normal basis theorem.)

BIX) (a) Let $A = k[X_1, \ldots, X_n]/\big(f(X_1, \ldots, X_n)\big)$, where k is a field. Assume, for each maximal ideal, $\mathfrak{p}$, of A, we have $(\operatorname{grad} f)(\mathfrak{p}) \neq 0$ (i.e., $(\forall\, \mathfrak{p})(\exists$ component of $\operatorname{grad} f$ not in $\mathfrak{p})$). Show that $\mathrm{Der}_k(A, A)$ is a projective A-module.

(b) Suppose now $A = k[X, Y]/(Y^2 - X^3)$, $\mathrm{char}(k) \neq 2, \neq 3$. Consider the linear map $A \amalg A \to A$ given by the matrix (X^2, Y); find generators for the kernel of this map.

(c) In the situation of (b), show that $\mathrm{Der}_k(A, A)$ is *not* projective over A.