MATH 594. SOLUTIONS TO FINAL EXAM

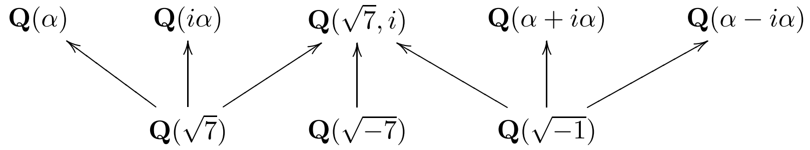
1. (20 pts) Work out the Galois group of $X^4 - 7$ over each of the following fields: $\mathbf{Q}$, $\mathbf{Q}(\sqrt{7})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-1})$. Determine the lattice of subfields for the case of $\mathbf{Q}$ as the base field.

Solution By Eisenstein's criterion, $f = X^4 - 7$ is irreducible over $\mathbf{Q}$. A splitting field has the form $K = \mathbf{Q}(\alpha, i)$ where $\alpha^4 = 7$ and $i^2 + 1 = 0$; the roots of f in K are $\pm\alpha$ and $\pm i\alpha$. Since $\mathbf{Q}(\alpha)$ has degree 4 and admits a real embedding, $i \notin \mathbf{Q}(\alpha)$. Thus, $[K : \mathbf{Q}] = 8$. The only possible automorphisms are those determined by $\alpha \mapsto i^r\alpha$ for $r \in \mathbf{Z}/4$ and $i \mapsto \pm i$. These are 8 options, so all must work. Letting σ be the automorphism which fixes i and sends α to $i\alpha$, and τ be the automorphism which fixes α and sends i to $-i$, we have $\sigma^4 = 1$, $\tau^2 = 1$, and $\tau\sigma\tau^{-1} = \sigma^3 = \sigma^{-1}$. That is, $\mathrm{Gal}(K/\mathbf{Q}) \simeq D_4$. The quadratic subfields correspond to the order 4 (i.e., index 2) subgroups. Such a subgroup must contain σ^2, so these are

$$\langle\sigma\rangle \simeq \mathbf{Z}/4, \ \langle\sigma^2, \tau\rangle \simeq \mathbf{Z}/2 \times \mathbf{Z}/2, \ \langle\sigma^2, \sigma\tau\rangle \simeq \mathbf{Z}/2 \times \mathbf{Z}/2.$$

The associated quadratic fixed fields are $\mathbf{Q}(i) \simeq \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\alpha^2) = \mathbf{Q}(\sqrt{7})$, and $\mathbf{Q}(i\alpha^2) \simeq \mathbf{Q}\sqrt{-7})$ (so the Galois group for the splitting field of $X^4 - 7$ over each of these quadratic fields is the indicated order 4 group mentioned above).

The order 4 subextensions correspond to the order 2 subgroups. The elements of order 2 in D_8 are τ, σ^2, and $\sigma^j\tau$. The fixed field of τ is $\mathbf{Q}(\alpha)$ and the fixed field of $\sigma^2\tau$ is $\mathbf{Q}(i\alpha)$, as one sees by inspection. The fixed field of $\sigma\tau$ is $\mathbf{Q}(\alpha + i\alpha)$ (as one sees by first averaging to make the guess, and then checking directly, for example), and likewise the fixed field of $\sigma^{-1}\tau$ is $\mathbf{Q}(\alpha - i\alpha)$. The fixed field of σ^2 is $\mathbf{Q}(\alpha^2, i) \simeq \mathbf{Q}(\sqrt{7}, \sqrt{-1})$. The lattice of intermediate fields between K and $\mathbf{Q}$ (omitting K and $\mathbf{Q}$ from the picture) is:



2. Recall from class that we have a natural isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n)^\times$ for any $n \geq 1$, where ζ_n is a primitive nth root of unity in some extension of $\mathbf{Q}$. In this problem, we work inside of a fixed algebraic closure $\overline{\mathbf{Q}}$.

(*i*) (10 pts) For n and m positive integers, with $n|m$, show that the natural diagram of groups

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) & \simeq & (\mathbf{Z}/m)^\times \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) & \simeq & (\mathbf{Z}/n)^\times \end{array}$$

commutes. Use this to show that $\mathbf{Q}(\zeta_a) \cap \mathbf{Q}(\zeta_b) = \mathbf{Q}$ if and only if $\gcd(a, b) = 1$ or 2.

(*ii*) (10 pts) Using the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/p^n)^\times$ for any prime p and any $n \geq 1$, along with the known structure of the group $(\mathbf{Z}/p^n)^\times$, show that $\mathbf{Q}(\zeta_{p^n})$ contains a unique subfield K of degree p^{n-1} over $\mathbf{Q}$ and that $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$.

Solution

(*i*) For any $s \in (\mathbf{Z}/m)^\times$, the sth power map on mth roots of unity restricts to the sth power map on the subgroup of nth roots of unity (and only depends upon $s \bmod n \in (\mathbf{Z}/n)^\times$). Keeping in mind how the map $\mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q}) \to (\mathbf{Z}/d)^\times$ is *defined* in terms of exponentiation on roots of unity, the commutativity of the diagram drops out.

If $d = \gcd(a, b)$, then $\mathbf{Q}(\zeta_d) \subseteq \mathbf{Q}(\zeta_a) \cap \mathbf{Q}(\zeta_b)$, so when this latter intersection is $\mathbf{Q}$ then $\mathbf{Q}(\zeta_d) = \mathbf{Q}$ and hence $d = 1$ or $d = 2$. For the converse, note that $\mathbf{Q}(\zeta_{2r}) = \mathbf{Q}(\zeta_r)$ for *odd* r, so if $\gcd(a, b) = 2$ then at least one of a or b is twice an odd number and hence by halving that index we don't change fields. Thus, for ths converse we may assume $\gcd(a, b) = 1$. By the Chinese Remainder Theorem, the ring map $\mathbf{Z}/(ab) \to \mathbf{Z}/a \times \mathbf{Z}/b$ is an isomorphism, so the induced map on unit groups is an isomorphism. But taking $m = ab$ and $n = a, b$ identifies this isomorphism with the natural product map

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{ab})/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\zeta_a)/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_b)/\mathbf{Q}).$$

Hence, this latter map is an isomorphism. It follows by inspection that the kernels of the two projections therefore generate all of $\mathrm{Gal}(\mathbf{Q}(\zeta_{ab})/\mathbf{Q})$, but these kernels are the fixed groups for the subfields $\mathbf{Q}(\zeta_a)$ and $\mathbf{Q}(\zeta_b)$, so the fixed group associated to the intersection field $\mathbf{Q}(\zeta_a) \cap \mathbf{Q}(\zeta_b)$ is the group generated by these two kernels. As this subgroup is the whole group, by the Galois correspondence this intersection must be $\mathbf{Q}$.

(*ii*) $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) = (\mathbf{Z}/p^n)^\times$, which is (canonically) a product of its *cyclic* p-Sylow subgroup (of order p^{n-1}) and the product of the other Sylow subgroups — a cyclic group of order $p-1$ (representing the canonical $(\mathbf{Z}/p)^\times$ quotient). Let K be the fixed field of the cyclic subgroup of order $p-1$. Then use the Fundamental Theorem of Galois Theory.

3. (20 pts) The problem works out some examples with quadratic fields.

(*i*) (8 pts) Construct a finite Galois extension $L/\mathbf{Q}(\sqrt{2})$ with $\mathrm{Gal}(L/\mathbf{Q}(\sqrt{2})) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$ and L *not* Galois over $\mathbf{Q}$ (prove it!).

(*ii*) (12 pts) Using that $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q}) \to (\mathbf{Z}/8)^\times$ is an isomorphism (proven in Problem 2), find all subfields of $\mathbf{Q}(\zeta_8)$, writing each quadratic subfield in the form $\mathbf{Q}(\sqrt{d})$ for an explicit squarefree integer d.

Solution

(*i*) Let $K = \mathbf{Q}(\sqrt{2})$. Take $L = K(\alpha, \beta)$ where $\alpha^2 = 3$ and $\beta^2 = \sqrt{2}$ (a splitting field of $(X^2-3)(X^2-\sqrt{2}) \in K[X]$). It is easy to check that 3, $\sqrt{2}$, and $\sqrt{2}/3$ are non-squares in K, so L is degree 4 over K with

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K(\alpha)/K) \times \mathrm{Gal}(K(\beta)/K) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2.$$

To see L is not Galois over $\mathbf{Q}$, note that it contains a root β of the irreducible $X^4 - 2 \in \mathbf{Q}[X]$, yet does not contain a splitting field of this polynomial since it does not contain a primitive 4th root of unity (indeed, L clearly has a real embedding).

(*ii*) As an abstract group $(\mathbf{Z}/8)^\times$ is isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/2$, so there are exactly 3 subfields of $\mathbf{Q}(\zeta)$ distinct from $\mathbf{Q}$ and $\mathbf{Q}(\zeta)$, each of degree 2 over $\mathbf{Q}$; here, $\zeta = \zeta_8$ has minimal polynomial X^4+1. One of these is $\mathbf{Q}(i)$ where $i = \zeta^2$ is a primitive 4th root of unity. This is the subgroup invariant under $-1 \in (\mathbf{Z}/8)^\times$. Another order 2 subgroup is the one generated by 3, for which $\alpha = \zeta + \zeta^3$ is invariant. Clearly α is not in $\mathbf{Q}$, so $\mathbf{Q}(\alpha)$ is the fixed field of $\langle 3 \rangle$, hence is quadratic over $\mathbf{Q}$, with $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ an order 2 group with generator induced by the action w of $-1 \in (\mathbf{Z}/8)^\times$ (as well as by the action of $5 \in (\mathbf{Z}/8)^\times$). To find its minimal polynomial, we compute the sum and product of its conjugate over $\mathbf{Q}$:

$$z + w(z) = \zeta + \zeta^3 + \zeta^{-1} + \zeta^{-3} = 0, \ \ zw(z) = (\zeta + \zeta^3)(\zeta^{-1} + \zeta^{-3}) = 2 + \zeta^2 + \zeta^{-2} = 2 + i - i = 2$$

(to compute the big sum by pure thought, recall ζ has minimal polynomial X^4+1), so z is a root of X^2-2. Hence, $\mathbf{Q}(\sqrt{2})$ is another such subfield, and $\mathbf{Q}(\sqrt{-2})$ must therefore be the third.

4. (20 pts) Give examples for each of the following, or indicate that no such example exists. In each case, provide brief justification.

(*i*) (4 pts) A finite field of order 30.

(*ii*) (4 pts) A field F which is abstractly isomorphic to a proper subfield $F' \subsetneq F$.

(*iii*) (4 pts) A Galois extension of $\mathbf{Q}$ with Galois group C_{13}.

(*iv*) (4 pts) A Galois extension of $\mathbf{F}_3$ with Galois group $\mathbf{Z}/2 \times \mathbf{Z}/2$.

(*v*) (4 pts) A field of characteristic zero which cannot be embedded into $\mathbf{C}$.

Solution

(*i*) Finite fields have prime power order, so no example exists.

(*ii*) $F = \mathbf{Q}(t)$, $F' = \mathbf{Q}(t^2)$, using $f(t^2) \mapsto f(t)$.

(*iii*) Since 13 divides $52 = 53 - 1$, $\mathbf{Q}(\zeta_{53})$ has cyclic Galois group of order 52. Take the unique subfield of degree 13 over $\mathbf{Q}$.

(*iv*) Galois extensions of finite fields are cyclic, so no such example exists.

(*v*) The field $K = \mathbf{Q}(X_i)$ on a set of indeterminates of cardinality larger than the size of $\mathbf{C}$. We cannot even embed K into $\mathbf{C}$ as a subset, let alone as subfield.

5. (20 pts) If K/k is an extension of fields, a k-*derivation* from K to K is a k-linear map $D : K \to K$ such that $D(xy) = xD(y) + yD(x)$ for all $x, y \in K$ (the *Leibnitz rule*).

(*i*) (5 pts) Prove that for any k-derivations $D_1, D_2 : K \to K$ and any elements $c_1, c_2 \in K$, $c_1D_1 + c_2D_2$ and $D_1 \circ D_2 - D_2 \circ D_1$ are k-derivations from K to K.

(*ii*) (5 pts) Applying the Leibnitz Rule to the identities $1 \cdot 1 = 1$ and $xx^{-1} = 1$ (for $x \neq 0$), conclude that $D(1) = 0$ and $D(x^{-1}) = -D(x)/x^2$ for any nonzero $x \in K$, and likewise show $D(x^n) = nx^{n-1}D(x)$ for all $n \geq 1$ and $x \in K$. Deduce that if $a \in K$ then two k-derivations $D_1, D_2 : K \to K$ coincide on $k(a) \subseteq K$ if and only if $D_1(a) = D_2(a)$.

(*iii*) (5 pts) If $K = k(T)$ for an indeterminate T, prove that the k-derivations $D : K \to K$ are precisely the operators $D_c : f \mapsto c\,f'(T)$ for varying $c \in K$ (hint: prove that $c \cdot \mathrm{d}/\mathrm{d}T$ is a derivation with value c on T, and use (*ii*)).

(*iv*) (5 pts) For any $a \in K$ and $f \in k[T]$, prove $D(f(a)) = f'(a)D(a)$ for any k-derivation $D : K \to K$. Conclude that if K/k is separable algebraic, then the only k-derivation $D : K \to K$ is $D = 0$.

Solution

(*i*) The case of $c_1D_2 + c_2D_2$ is easy, and for the "commutator" we compute

$$D_1(D_2(xy)) - D_2(D_1(xy)) = D_1(xD_2(y) + yD_2(x)) - D_2(xD_1(y) + yD_1(x)),$$

which we expand as

$$\begin{aligned} &D_1(x)D_2(y) + xD_1(D_2(y)) + D_1(y)D_2(x) + yD_1(D_2(x)) \\ -&D_2(x)D_1(y) - xD_2(D_1(y)) - D_2(y)D_1(x) - yD_2(D_1(x)), \end{aligned}$$

and upon cancelling we get

$$x(D_1(D_2(y)) - D_2(D_1(y))) + y(D_1(D_2(x)) - D_2(D_1(x)),$$

as desired. The k-linearity aspect is trivial.

(*ii*) Since $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = 2D(1)$, we get $D(1) = 0$. Thus, for $x \neq 0$,

$$0 = D(1) = D(x \cdot x^{-1}) = xD(x^{-1}) + x^{-1}D(x),$$

from which we see $D(x^{-1}) = -D(x)/x^2$. The identity $D(x^n) = nx^{n-1}D(x)$ for $n \geq 1$ and $x \in K$ is easy via induction on n with the help of the Leibnitz Rule.

If $D_1(a) = D_2(a)$, then by the power rule $D_1(a^n) = D_2(a^n)$ for any $n \geq 1$, so by k-linearity we see that the D_j's coincide on $k[a]$. By the inversion rule, the D_j's therefore agree on reciprocals of nonzero elements in $k[a]$, and so by the Leibnitz Rule (write an element in $k(a)$ as $x \cdot y^{-1}$ for $x, y \in k[a]$ with $y \neq 0$) we see that the D_j's agree on $k(a)$.

(*iii*) The operator $\mathrm{d}/\mathrm{d}T$ is trivially a k-derivation from $K = k(T)$ to itself, so $D_c = c \cdot \mathrm{d}/\mathrm{d}T$ is as well for any $c \in K$. This derivation has value c at T, so for any k-derivation $D : K \to K$ we see that for $c = D(1)$, the k-derivations D and D_c agree on T. Thus, by (*ii*), we get $D = D_c$.

(*iv*) Since D is k-linear, if $f = \sum c_jT^j$ with $c_j \in k$ then by the power rule

$$D(f(a)) = \sum c_jD(a^j) = \sum_{j \geq 1} jc_ja^{j-1}D(a) = f'(a)D(a).$$

If K/k is separable algebraic, then any $a \in K$ satisfies $f(a) = 0$ for some $f \in k[T]$ with $f'(a) \neq 0$ (namely, take f to be the minimal polynomial of a over k). Then $0 = D(0) = D(f(a)) = f'(a)D(a)$, so $D(a) = 0$ since $f'(a) \neq 0$. Thus, $D = 0$ when K/k is separable algebraic.

6. (20 pts) We say that a polynomial $f \in k[X]$ over a field k is *additive* if $f(U) + f(V) = f(U + V)$ in $k[U, V]$.

(*i*) (5 pts) If k has characteristic zero, prove that an additive polynomial in $k[X]$ is precisely one of the form $f = cX$ with $c \in k$.

(*ii*) (10 pts) If k has positive characteristic p, show that $f \in k[X]$ is additive if and only if $f = \sum c_jX^{p^j}$.

(*iii*) (5 pts) We say that a polynomial $f(X)$ is *multiplicative* if $f(U)f(V) = f(UV)$ in $k[U, V]$. In any characteristic, prove that the multiplicative polynomials are the zero polynomial and the monomials $f = X^n$ with $n \geq 0$.

Solution

(i) Sending $U, V \mapsto 0$, we see that $f(0) = 0$ for an additive polynomial in any characteristic. It remains to show that in characteristic zero, f cannot have leading term cX^n with $n > 1$. In such cases, $f(U + V)$ has top degree monomials of total degree n, coming from $c(U + V)^n$. The binomial expansion with $n > 1$ provides nonzero cross terms in $f(U + V) \in k[U, V]$ since the binomial coefficients are nonzero in k. The presence of such cross terms is incompatible with an equality $f(U + V) = f(U) + f(V)$.

(ii) By looking in total degree r, we see that for any $r > 0$ with X^r appearing in f, we must have $(U + V)^r = U^r + V^r$. We want to show that this can only happen if r is a power of p (the converse is trivial). If we can deduce that r is divisible by p, then by considering the identity inside of the field $k(U, V)$ we could extract pth roots so as to replace r with r/p, and by induction on r we would get the desired result.

Thus, we must show that if $r > 1$ is not divisible by p then $(U + V)^r \neq U^r + V^r$ in $k[U, V]$. If such an equality does hold, taking partial derivatives with respect to U yields $r(U + V)^{r-1} = rU^{r-1}$, so by cancelling the nonzero $r \in k$ we would get $(U + V)^{r-1} = U^{r-1}$ in $k[U, V]$. By expanding out $(U + V)^{r-1}$ if $r > 1$, we get a contradiction by noticing that V^{r-1} appears on the left side without cancelling out.

(iii) We may assume f is nonzero. If f has leading term cU^n with $n \geq 0$, then clearly $(cU^n)(cV^n) = c(UV)^n$, so $c = 1$. Since $f(UV)$ is a polynomial in powers U^jV^j, there cannot be term in f other than the lead term U^n since otherwise in the product $f(U)f(V)$ there would be nonzero cross terms with unequal exponents, contradicting an equality with $f(UV)$.