Math 5055: Advanced Algebra II

Assignment 4

Solutions

Galois groups

1. **Determine the Galois groups of the following polynomials over the fields indicated.**

   (a) $x^4 - 5$ **over** $\mathbb{Q}$**; over** $\mathbb{Q}[\sqrt{5}]$**; over** $\mathbb{Q}[\sqrt{-5}]$**.**

   The splitting field of $x^4 - 5$ is $\mathbb{Q}[i, \sqrt[4]{5}]$, where of course $i = \sqrt{-1}$. Thus its Galois group over $\mathbb{Q}$ has order 8. It acts transitively on the four roots $\sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}, -i\sqrt[4]{5}$. The only transitive subgroup of S_4 of order 8 is the dihedral group D_4. It acts in the "obvious" way on the square with vertices $\{\sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}, -i\sqrt[4]{5}\}$.

   The polynomial $x^4 - 5$ factors over $\mathbb{Q}[\sqrt{5}]$ as $(x^2 - \sqrt{5})(x^2 + \sqrt{5})$. Thus the Galois group, now of order 4, does not act transitively: rather, it breaks the roots into the two orbits $\{\pm\sqrt[4]{5}\}$ and $\{\pm i\sqrt[4]{5}\}$. It is thus the Klein-4 subgroup of D_4 generated by complex conjugation and the transposition $\sqrt[4]{5} \leftrightarrow -\sqrt[4]{5}$.

   The following products of roots equal $\sqrt{-5}$, and so are fixed by the Galois group of $x^4 - 5$ over $\mathbb{Q}[\sqrt{-5}]$:

   $$\sqrt[4]{5} \cdot i\sqrt[4]{5}, \qquad -\sqrt[4]{5} \cdot -i\sqrt[4]{5}.$$

   These correspond to two oppositve edges of the square with vertices $\{\sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}, -i\sqrt[4]{5}\}$. So we are looking for an order-4 subgroup of D_4 which may exchange these two edges, but does not mix them with the other two edges. There is one such subgroup. It is the Klein-4 subgroup whose nontrivial elements are:

   $$\sqrt[4]{5} \leftrightarrow i\sqrt[4]{5} \text{ and } -\sqrt[4]{5} \leftrightarrow -i\sqrt[4]{5},$$
   $$\sqrt[4]{5} \leftrightarrow -i\sqrt[4]{5} \text{ and } -\sqrt[4]{5} \leftrightarrow i\sqrt[4]{5},$$
   $$\sqrt[4]{5} \leftrightarrow -\sqrt[4]{5} \text{ and } i\sqrt[4]{5} \leftrightarrow -i\sqrt[4]{5}$$

   This subgroup acts transitively, and so $x^4 - 5$ is irreducible over $\mathbb{Q}[\sqrt{-5}]$.

   (b) $x^3 - x - 1$ **over** $\mathbb{Q}$**; over** $\mathbb{Q}[\sqrt{-23}]$**.**

   The polynomial is irreducible over $\mathbb{Q}$: it is cubic, and so to check irreducibility is suffices to check that it has no roots; it is monic over $\mathbb{Z}$, and so its rational roots are integers; but if $|x| \geq 2$, then $|x^3| > |x| + |1| \geq |x - 1|$, and $x = 0, 1, -1$ are not roots by direct checking. Since the polynomial is irreducible, the Galois group is a transitive subgroup of S_3.

   The discriminant of $x^3 - x - 1$ is $D = -4(-1)^3 - 27(-1)^2 = -23$. This is not a square in $\mathbb{Q}$, and so the Galois group is S_3, which has order 6. Thus the splitting field of $x^3 - x - 1$ has degree 6 over $\mathbb{Q}$.

The square root of the discriminant $\Delta = \sqrt{D} = \sqrt{-23}$ is an element of the splitting field of $x^3 - x - 1$. Thus this splitting field has degree $6/2 = 3$ over the degree-2 extension $\mathbb{Q}[\sqrt{-23}]$ of $\mathbb{Q}$. So the Galois group has order 3, and hence is $A_3 \subset S_3$. This is transitive, and so $x^3 - x - 1$ is irreducible over $\mathbb{Q}[\sqrt{-23}]$.

(c) $x^4 + 3x^3 + 3x - 2$ **over** $\mathbb{Q}$**.**

Set $f(x) = x^4 + 3x^3 + 3x - 2$. The resolvent cubic of f is

$$g(x) = x^3 + 0x^2 + (3 \cdot 3 - 4 \cdot (-2))x - 3^2 \cdot (-2) + 0 - 3^2 = x^3 + 17x + 9.$$

This has only one real root — its derivative is always positive — and the real root is strictly between $x = -1$ and $x = 0$ (since $g(-1) = -9 < 0$ and $g(0) = 9 > 0$). In particular, g has no integral roots, and hence no rational roots since g is monic over $\mathbb{Z}$. But g is cubic, and so the lack of rational roots implies that it is irreducible over $\mathbb{Q}$.

Since 3 is prime and g has exactly $3 - 2 = 1$ real root, the Galois group of g is S_3. In particular, the splitting field of g is a degree-6 extension of $\mathbb{Q}$. Assuming f is irreducible, it follows that the Galois group of f is S_4.

Is f irreducible? Note that f is quartic, so if it is to factor, then it must factor as either (quadratic)·(quadratic) or (cubic)·(linear).

In the former case, the Galois group of f would be $\mathbb{Z}/2 \times \mathbb{Z}/2$ (assuming the two quadratics factors have different splitting fields; if they have the same splitting field, or if they factor further, then the Galois group would be smaller than $\mathbb{Z}/2 \times \mathbb{Z}/2$). But the splitting field of g is contained within the splitting field of f, and so the Galois group of f surjects onto the Galois group of g, which has order 6. So (quadratic)·(quadratic) is ruled out.

What about (cubic)·(linear)? Then f has a rational root, and since f is monic over $\mathbb{Z}$, that root must be integral. Let's test some values of f.

$$\begin{gathered} f(-x) > |x|^3 > 0 \text{ if } x < -4, \\ f(-4) = 64 - 48 - 12 - 2 > 0, \\ f(-3) = 81 - 81 - 9 - 2 < 0, \\ f(-2) = 16 - 18 - 3 - 2 < 0, \\ f(-1) = 1 - 3 - 3 - 3 < 0, \\ f(0) = 0 + 0 + 0 - 2 < 0, \\ f(1) = 1 + 3 + 3 - 2 > 0, \\ f(x) > |x|^4 \text{ if } x > 1. \end{gathered}$$

So f has real roots in the intervals $(-4, -3)$ and $(0, 1)$, but no integer roots, and hence is irreducible.

(Although we don't need it, we remark that f cannot have more than two real roots. There are many ways to see this. One is that g has complex roots, and so f must as well: the splitting field of f cannot be contained in $\mathbb{R}$, since it contains the splitting field of g. Another is to use derivatives: $f'(x) = 4x^3 + 6x^2 + 3$ has only one real root since $f''(x) = 12x^2 + 6$ is always positive, but the derivative of a function has a real root between any two real roots of the function.)

(d) $x^5 - 6x + 3$ **over** $\mathbb{Q}$**.**

The polynomial is irreducible by Eisenstein's criterion, and it has three real roots (confirmed with a graphing calculator). So its Galois group is S_5.

2. **Which roots of unity are contained in the following fields?**

$$\mathbb{Q}[\sqrt{-1}], \quad \mathbb{Q}[\sqrt{2}], \quad \mathbb{Q}[\sqrt{3}], \quad \mathbb{Q}[\sqrt{5}], \quad \mathbb{Q}[\sqrt{-2}], \quad \mathbb{Q}[\sqrt{-3}].$$

These fields are all quadratic extensions of $\mathbb{Q}$, and so their elements are (either rational or) quadratic over $\mathbb{Q}$. Suppose ξ is a primitive ℓth root of unity. Then the degree of ξ is the Euler totient function $\varphi(\ell) = \#(\mathbb{Z}/\ell)^\times$. By the Chinese remainder theorem, $\varphi(mn) = \varphi(m)\varphi(n)$ if m and n are coprime, and an easy calculation shows $\varphi(p^n) = p^{n-1}(p-1)$ if p is prime. From this one quickly finds that the only solutions to $\varphi(\ell) = 2$ are $\ell = 3, 4, 6$.

The fourth roots of unity are $\pm\sqrt{-1}$, and are contained in $\mathbb{Q}[\sqrt{-1}]$. The third and sixth roots of unity are $\pm\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ and are contained in $\mathbb{Q}[\sqrt{-3}]$. Other than these cases, the only roots of unity in a quadratic extension of $\mathbb{Q}$ are ± 1 (which are in all extensions of $\mathbb{Q}$).

3. **Let $\mathbb{K} \subset \mathbb{L}$ be an extension of finite fields, i.e. $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{L} = \mathbb{F}_{q^m}$ for some prime power $q = p^n$. Show that both the Trace $T^{\mathbb{L}}_{\mathbb{K}} : \mathbb{L} \to \mathbb{K}$ and the Norm $N^{\mathbb{L}}_{\mathbb{K}} : \mathbb{L} \to \mathbb{K}$ are surjective.**

The Galois group of $\mathbb{K} \subset \mathbb{L}$ is cyclic of order m generated by $\phi : v \mapsto v^q$. Recall that $T = I + \phi + \phi^{\circ 2} + \cdots + \phi^{\circ(m-1)}$, where I denotes the identity operator. Consider the 2-periodic exact sequence

$$\cdots \to \mathbb{L} \xrightarrow{T} \mathbb{L} \xrightarrow{I-\phi} \mathbb{L} \xrightarrow{T} \mathbb{L} \xrightarrow{I-\phi} \mathbb{L} \to \ldots.$$

By Hilbert's theorem 90, this sequence is exact at the "$\xrightarrow{I-\phi}\ \mathbb{L}\ \xrightarrow{T}$" entries. But it is a sequence of finite abelian group, and so by counting the sizes of kernels and images, the sequence must be exact also at the "$\xrightarrow{T}\ \mathbb{L}\ \xrightarrow{I-\phi}$" entries. (To wit: Hilbert's theorem 90 implies in particular that $\#\operatorname{im}(I-\phi) = \#\ker(T)$. But the first isomorphism says implies that $\#\operatorname{im}(I-\phi) \times \#\ker(I-\phi) = \#\mathbb{L} = \#\operatorname{im}(T) \times \#\ker(T)$.)

In particular, the image of T is precisely the kernel of $I-\phi$, or in other words the fixed points of ϕ. But the extension is Galois, and so the fixed points of ϕ are precisely $\mathbb{K}$.

Exactly the same argument works for N, thought of as a homomorphism with domain $\mathbb{L}^\times$ (obviously $0 = N(0)$, and so we might as well excuse it from the table). Writing the group law on $\mathbb{L}^\times$ multiplicatively, we have $N = I \times \phi \times \phi^{\circ 2} \times \cdots \times \phi^{\circ(m-1)} : \mathbb{L}^\times \to \mathbb{L}^\times$, and we also consider $I \div \phi : \mathbb{L}^\times \to \mathbb{L}^\times$. Then Hilbert's theorem 90 says that the sequence

$$\cdots \to \mathbb{L}^\times \xrightarrow{N} \mathbb{L}^\times \xrightarrow{I\div\phi} \mathbb{L}^\times \xrightarrow{N} \mathbb{L}^\times \xrightarrow{I\div\phi} \mathbb{L}^\times \to \ldots$$

is exact at alternating entries, and hence exact at the other half of the entries by counting. In other words, the image of N is all of the kernel of $I \div \phi : \mathbb{L}^\times \to \mathbb{L}^\times$, i.e. all of the fixed points of ϕ, i.e. all of $\mathbb{K}^\times$.

Representations of finite groups

4. **Given a group G, let $G' < G$ denote its *commutator subgroup*, i.e. the subgroup generated by elements of the form $ghg^{-1}h^{-1}$.**

   (a) **Show that G' is normal in G, and that the quotient G/G' is abelian.**
   Indeed: G' is *characteristic*, i.e. preserved by all automorphisms of G. Normality is simply that it is preserved by inner automorphisms.

(b) **Show that the one-dimensional representations of G are in bijection with the one-dimensional representations of G/G'.**

For any group A, restriction along the surjection $G \to G/G'$ gives an injection $\hom(G/G', A) \to \hom(G, A)$. If A is abelian, then any homomorphism $\rho : G \to A$ will trivialize on G', and hence factor through G/G', and so the injection $\hom(G/G', A) \to \hom(G, A)$ is a bijection.

But a one-dimensional representation (over a field $\mathbb{F}$) is nothing but a homomorphism into $\mathrm{GL}(1, \mathbb{F}) = \mathbb{F}^\times$.

5. **Suppose that A is a finite abelian group and $\mathbb{F}$ is algebraically closed. Show that a representation of A over $\mathbb{F}$ is irreducible if and only if it is 1-dimensional.**

One-dimensional vector spaces have no proper sub-vector spaces, and so one-dimensional representations of any group are automatically irreducible. The only fact to prove is that all if A is abelian, then all of its irreps are one-dimensional. But this follows from the fact that, over an algebraically closed field, any finite set of commuting operators (on a finite-dimensional vector space) has a common eigenvector.

To spell it out, let $a_1, \ldots, a_n$ be a set of generators for A. Let V be a finite-dimensional representation of A. We will show that if V is not one-dimensional, then it has a proper A-invariant subspace. Abusing notation, write $a_1, \ldots, a_n$ also for their images in $\mathrm{GL}(V)$. Now, using that $\mathbb{F}$ is algebraically closed, choose an eigenvalue λ of a_1. The corresponding eigenspace $\ker(a_1 - \lambda)$ is nonzero and invariant under $a_2, \ldots, a_n$ (since the operators commute). So either V is reducible, in which case we're done, or $a_1 = \lambda$ acts by a scalar. Now repeat for a_2, etc., and discover that all of the a_is, and hence all of A, are acting by scalars. But then V splits as a direct sum of $\dim(V)$ many copies of the same scalar representation, and so $\dim(V) = 1$.

6. **Suppose that G is a group, with centre $Z(G)$. Suppose that $(V, \rho_V : G \to \mathrm{GL}(V))$ is an irreducible representation of G over an algebraically closed field $\mathbb{F}$. Show that if $c \in Z(G)$ then $\rho_V(c)$ is a scalar multiple of the identity operator. In other words, show that ρ restricts to a homomorphism $Z(G) \to \mathbb{F}^\times$. This homomorphism is called the *central character* of the representation (V, ρ_V).**

Conclude that, if a finite group G admits a faithful irreducible representation, then its centre must be cyclic.

Since V is irreducible, by Schur's lemma the only linear endomorphisms of V which commute with all of $\rho_V(G)$ are scalars. (In general, they are "scalars" in some division ring over $\mathbb{F}$, but $\mathbb{F}$ is algebraically closed.) But $Z(G)$ commutes with all of G, and so $\rho_V(Z(G))$ commutes with all of $\rho_V(G)$.

For the conclusion, note that a finite subgroup of $\mathbb{F}^\times$ is necessarily cyclic. (Since otherwise there would be too many solutions to an equation of the form $x^n = 1$.)

7. **Let p be a positive prime, P a p-group (i.e. a group of order a power of p), and $\mathbb{F}$ a field of characteristic p. Prove that the only irreducible representation of P over $\mathbb{F}$ is the trivial one.**

Hints: P contains a central element c of order p. Use exercise 6.

Suppose (V, ρ) is an irrep of P. By the previous exercise, the centre of P acts by scalars. Let $c \in Z(P)$ have order p. Then $x = \rho(c)$ solves $x^p = 1$. But since we are in characteristic p, the

only solution to $x^p = 1$ is $x = 1$. In other words, c acts trivially, and so the representation ρ factors through $P/\langle c \rangle$.

In general, if G is a group with a normal subgroup H, and if V is a representation of G/H, then V is irreducible over G/H if and only if it is irreducible after pulling back to G. So we have an irrep of $P/\langle c \rangle$. This irrep is trivial by induction on the order of P.