VIGRE Algebra QR Review, September 30, 2002

Summary of Session

Theoretical points: If two fields K and K' are isomorphic, then the splitting fields of two sets of polynomials that correspond under the isomorphism are also isomorphic (but not necessarily in a unique way). If one has two possibly different roots θ and θ' of the same irreducible polynomial $f = f(x) \in K[x]$, then $K[\theta] \cong K[\theta']$ (both are $\cong K[x]/(f)$). This isomorphism extends to an isomorphism of splitting fields. If θ and θ' lie in the same splitting field, this will be an automorphism of that splitting field. This automorphism extends to any further normal field extension. Thus, the K-automorphism group of any normal algebraic field extension L of K acts transitively on the roots of a polynomial irreducible over K. Conversely, if a polynomial has all distinct roots and the automorphism group of an extension containing them acts transitively on them, the polynomial is irreducible. The reason is that if it factors as $g(x)h(x)$, then the roots of g are stable under the action, and so are the roots of h, contradicting the transitivity of the action. Thus, a polynomial with distinct roots is irreducible over K if and only if its Galois group over K acts transitively on the roots.

The *cyclotomic* polynomials are defined recursively as follows. Let $\phi_1(x) = x - 1$, and, if $n \geq 1$, let $\phi_n(x) = (x^n - 1)/\prod_d \phi_d(x)$, where d runs through integers such that $d|n$ and $1 \leq d < n$. Thus, $\phi_2(x) = (x^2 - 1)/(x - 1) = x + 1$, $\phi_3(x) = (x^3 - 1)/(x - 1) = x^2 + x + 1$, $\phi_4(x) = (x^4 - 1)/\big((x - 1)(x + 1)\big) = x^2 + 1$, $\phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$, and $\phi_6(x) = (x^6 - 1)/\big((x - 1)(x + 1)(x^2 + x + 1)\big) = x^2 - x + 1$. In the first few, e.g., for $n \leq 104$, all coefficients $\in \{-1, 0, 1\}$ but this eventually fails. One shows by induction that the roots of $\phi_n(x)$ are precisely the primitive n th roots of unity. A somewhat subtle argument that uses reduction to characteristic $p > 0$ can be used to show that these polynomials are irreducible over $\mathbb{Q}$. The degree of ϕ_n is given by the Euler Φ function: $\Phi(n)$ is the order of the multiplicative group of invertible integers mod n. The elements are in bijective correspondence with the integers in $\{1, \ldots, n - 1\}$ that are relatively prime to n. If n has prime factorization $p_1^{k_1} \cdots p_r^{k_r}$ with the p_j distinct positive prime integers, then $\Phi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$. Fix a primitive n th root of unity, say θ. Then the splitting field of $x^n - 1$ over $\mathbb{Q}$ is $\mathbb{Q}[\theta]$ (the other roots of $x^n - 1$ are powers of θ). Since the irreducible equation of θ is $\phi_n(x)$, the splitting field has degree $\Phi(n)$. There will be an automorphism σ_i of the splitting field taking θ to θ^i for each integer i relatively prime to n: two values of i give the same automorphism if and only if they are congruent modulo n. Clearly, $\sigma_j \circ \sigma_i$ maps θ to $\sigma_j(\theta^i) = (\sigma_j(\theta))^i = ((\theta)^j)^i = \theta^{ij} = \sigma_{ij}(\theta)$. This gives an isomorphism of the multiplicative group in $\mathbb{Z}/n\mathbb{Z}$ with the Galois group of $x^n - 1$ over $\mathbb{Q}$. Note that it is canonical: σ_i maps all primitive n th roots of unity to their i th powers.

Facts about irreducibility. Let A be a unique factorization domain with fraction field F. An element of $A[x]$, where x is a variable, is irreducible if and only if it is irreducible over $F[x]$ (this uses Gauss' lemma) and the set of all nonzero coefficients has no common factor in A. Now suppose that one has a polynomial G in $A[x]$ with all coefficients relatively prime, that p is a prime element of A, that the leading coefficient is not divisible by p, but that all other coefficients are divisible by p. If the constant term is not divisible by p^2, the polynomial is irreducible over both $A[x]$ and $F[x]$. This is called Eisenstein's criterion.[1]

Solutions to various problems were presented as follows (these are all from the list for this week, unless otherwise indicated).

1. (Not a QR problem) Show that the only $\mathbb{Q}$-automorphism of $\mathbb{Q}[r]$, where r is the real cube root of 2, is the identity. (Failure of Galois theory for extensions that are not normal.)

Solution. Any automorphism must map the cube root of 2 to a cube root of 2: since two of the three cube roots of 2 are complex numbers, there is only one cube root of 2 in $\mathbb{Q}[r]$. It is therefore fixed, and since it generates $\mathbb{Q}[r]$ over $\mathbb{Q}$, the automorphism must be the identity.

3. Prove that A_6 (the alternating group in S_6) has no subgroup of order $72 = 6 \cdot 4 \cdot 3$. You may assume that A_6 is simple.

Solution. If A_6 had a subgroup of order 72 it would have index $(6{\cdot}5{\cdot}4{\cdot}3{\cdot}2/2)/(6{\cdot}4{\cdot}3) = 5$. The left action on left cosets by multiplication, which is transitive, gives a non-trivial map of A_6 in S_5. Since the kernel is a normal subgroup and cannot be the whole group, it must be trivial. But this implies that A_6 embeds in S_5, a contradiction, since $6!/2 = 3 \cdot 5! > 5!$. (The same argument shows that A_n cannot have a subgroup of index $n-1$ for $n \geq 5$. A related argument shows that if a normal group G has a subgroup of index p, then $|G|$ cannot be divisible by any prime greater than p (G embeds in S_p). In particular, G cannot have subgroups of index p and of index q where $p < q$ are prime.)

4. Find the splitting field K of the polynomial $x^4 - 7x^2 + 10$ over the field $\mathbb{Q}$ of rational numbers. Describe the Galois group G of K over $\mathbb{Q}$. Illustrate the fundamental correspondence of Galois theory in this example by finding all subgroups of G, all intermediate fields between $\mathbb{Q}$ and K, and describing their relationship. Which intermediate fields are normal extensions of $\mathbb{Q}$?

Solution. The equation factors $(x^2-2)(x^2-5)$ and so the splitting field is $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$. To see that $\sqrt{5}$ in not in $\mathbb{Q}[\sqrt{2}]$, we use the following trick. Suppose that $\sqrt{5} = a + b\sqrt{2}$ where a and b are rational. Since $\mathbb{Q}[\sqrt{2}]$ has an automorphism that sends $\sqrt{2}$ to $-\sqrt{2}$ that will extend to K, and since the roots of $x^2 - 5$ must be stable under this automorphism, we see that $a - b\sqrt{2}$ must be either $\sqrt{5}$ or $-\sqrt{5}$. In the first case $b = 0$, contradicting the irrationality of $\sqrt{5}$. In the second case, $a = 0$, and we find that $\sqrt{5/2} = b$ must be rational, a contradiction. (The square of a nonzero rational number written in lowest terms is again in lowest terms, and every prime that occurs in either the numerator or the denominator must occur with an even exponent.) It follows that we have one quadratic extension followed by another, and the degree will be four. The Galois group must consist of permutations of $\{\sqrt{2}, -\sqrt{2}, \sqrt{5}, -\sqrt{5}\}$, but each permutation stabilizes both the set

[1]Think over $(A/pA)[x]$. The polynomial becomes cx^d. This can only factor into two polynomials with constant term 0. This means that in a factorization of G over $A[x]$, both factors must have constant term divisible by p, and so the product of the constant terms will be divisible by p^2. $\square$

$\{\sqrt{2}, -\sqrt{2}\}$ and the set $\{\sqrt{5}, -\sqrt{5}\}$. There are only four permutations with this property: the identity, the permutation σ that fixes $\sqrt{5}$ and interchanges the square roots of 2, the permutation τ that fixes $\sqrt{2}$ and fixes the square roots of 5, and the composition $\sigma \circ \tau = \tau \circ \sigma$, which sends each of $\sqrt{2}$, $\sqrt{5}$ to its negative. The group is therefore the Klein 4-group, which is the abelian group consisting of the identity and three elements of order two: the product of any two distinct elements of order two is the third. This group may also be described as $\mathbb{Z}_2 \times \mathbb{Z}_2$. All the intermediate field extensions are normal, since all subgroups of an abelian group are normal. The strictly intermediate fields correspond to the three subgroups of order two: one is the fixed field of σ, which is $\mathbb{Q}[\sqrt{5}]$, one is the fixed field of τ, which is $\mathbb{Q}[\sqrt{2}]$, and one is the fixed field of $\sigma \circ \tau$, which is $\mathbb{Q}[\sqrt{10}]$.

5. Consider the extension of fields $L = \mathbb{C}(X) \supseteq \mathbb{C}(X^2 + \dfrac{1}{X^2}) = K$, where X is a variable, and $\mathbb{C}(X)$ denotes the field of rational functions in X.

(a) Show that this is a Galois extension of degree 4, with Galois group $G = \mathrm{Gal}\,(L/K)$ generated by the two automorphisms σ and τ such that $\sigma(X) = -X$ and $\tau(X) = 1/X$.

(b) Find the minimal polynomial of X over K.

(c) Find explicitly all intermediate fields lying between L and K, and find the subgroup to which each corresponds under the Galois correspondence.

Solution. Let $t = X^2 + 1/X^2$. Then clear denominators and collect terms to get that $X^4 - tX^2 + 1 = 0$, so that X is a root of $Z^4 - tZ^2 + 1$, as are the elements $-X, 1/X, -1/X$. It is clear the field extension is at most degree 4, and that σ, τ are in the automorphism group, as is $\sigma \circ \tau = \tau \circ \sigma$. Therefore, we must have that the degree is 4, and the entire Galois group must be $\sigma, \tau, \sigma \circ \tau$, along with the identity. This is a commutative group with every element except the identity of order two, i.e., a Klein 4-group as in problem 4. The fact that there are four automorphisms shows that the order of the extension is at least 4, and this shows that the equation we have given is irreducible. Another way to look at it is that the roots of the equation are X, $-X$, $1/X$, and $-1/X$, and the automorphisms can be used to map X to each of these. Since the Galois group acts transitively on the roots, the equation must be irreducible. A third method is to view it as a polynomial in the polynomial ring $\mathbb{C}[Z, t]$. It is irreducible over $\mathbb{C}(Z)[t]$ because it is linear in t, and over $\mathbb{C}[Z][t]$ because the coefficients $-Z^2$, $Z^4 + 1$ have no common factor (cf. the remarks on irreducibility at the beginning, third paragraph). Therefore it is also irreducible over $\mathbb{C}(t)[Z]$. There will be three strictly intermediate fields, all normal (as in the preceding problem), and they are the fixed fields of σ, τ, and $\sigma \circ \tau$, which are $\mathbb{C}(X^2)$, $\mathbb{C}(X + \frac{1}{X})$ and $\mathbb{C}(X - \frac{1}{X})$, respectively. (Note that in the latter two the square of the generator is $t \pm 2$, so that these do contain t.)

6. (Not a QR problem) Show that for any prime integer $p > 0$, the symmetric group on p elements is generated by any pair of elements consisting of a 2-cycle and a p-cycle. Conclude that a free group on two or more elements cannot be solvable.

Solution Suppose the 2-cycle is $(x_1 \;\; x_2)$. There will be a power of the p-cycle that sends x_1 to x_2 (this is where we are using that p is prime) and we may replace the p-cycle by this power. We may therefore assume that the elements are numbered so that the p-cycle is $(x_1\ x_2\ \dots\ x_p)$. Thus, there is no loss of generality in assuming that the 2-cycle is $a = (1\ 2)$ while the p-cycle is $b = (1\ 2\ \dots\ p)$. Then each $b^k a(b^k)^{-1}$ is a conjugate of a and also a 2-cycle. Since b^k sends 1 to $k+1$ (mod p), its inverse sends $k+1$ to 1, a maps 1 to 2, and then b^k maps 2 to $k+2$ (mod p). Thus, $b^k ab^{-k}$ is a 2-cycle that sends $k+1$ to $k+2$, and so it must be $(k+1\ \ k+2)$. By letting k take on the values $0, 1, \dots, p-2$ we get all of the transpositions $(1\ 2), (2\ 3), \dots, (p-1\ \ p)$. These generate S_p. (Informal proof: we can arrange the objects in a row any way we please by switching the one we want leftmost with its immediate neighbor repeatedly until it is where we want it, next repeating to get the object we want second in from the left where it is supposed to be, and so on.) The final statement follows because a free group with two or more generators can be mapped onto S_5 (or S_p for any prime $p \geq 5$), since it can be mapped onto any group with two generators. If the free group on two or more generators were solvable, then S_5 would be solvable, a contradiction.

7. Find the Galois group of the splitting field of $f(x) = x^5 - 6x + 3$ over the field of rational numbers.

Solution. The polynomial is irreducible by Eisenstein's criterion, since all of the coefficients except the leading coefficient are divisible by 3, but the constant term is not divisible by 9. Adjoining one root produces a field extension of degree 5, and so 5 divides the order of the Galois group. The Galois group is a subgroup of S_5 (permutations of the roots) that contains an element of order 5.

The derivative f' is $5x^4 - 6$, which has two roots, at $x = \pm(6/5)^{1/4}$, and so f increases until the first of these, then decreases, and then increases beyond the second root. Also, $x^5 - 6x + 3$ is negative for $x \ll 0$, is positive at $x = 0$, is negative at $x = 1$ and is positive for $x \gg 0$. It follows that this polynomial has precisely three real roots, and therefore it has two complex roots, which must be complex conjugates. Complex conjugation, restricted to the splitting field of f, gives an automorphism that fixes 3 of the roots of f while interchanging the other two. Thus, the Galois group of f is a subgroup of S_5 that contains both a 5-cycle and a 2-cycle. By the preceding problem, it must be all of S_5. Note that it follows that the given equation cannot be solved by radicals.

Problem 2. from the list of September 23 revisited, where the group generated by a primitive n th root of unity θ acts on $F = \mathbb{C}(x_1, \dots, x_n)$ so that θ maps x_i to $\theta^i x_i$. If one has somehow guessed that the invariant field is generated by x_1^n, $x_2/x_1^2, x_3/x_1^3, \dots, x_{n-1}/x_1^{n-1}$, and x_n, one can prove that one has all the invariants using Galois theory. Let K be the field generated by the specified invariants. We have that $K \subseteq F^G \subseteq F$. Now $[F : F^G] = n$, because a group of order n is acting faithfully. It suffices to show that $[F : K] \leq n$. But it is easy to see that $K(x_1) = F$, and that $[F : K] \leq n$ because x_1 is the n th root of $x_1^n \in K$.