These are analogues of the cubic resolvent used in the previous sections to determine the Galois group of quartic polynomials. These resolvent polynomials have rational coefficients and have as roots certain combinations of the roots of $f(x)$ (similar to the combinations $(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$ for the cubic resolvent). One then determines the factorization of these resolvent polynomials to obtain information on the Galois group of $f(x)$ — for example the existence of a linear factor implies the Galois group lies in the stabilizer in S_n of the combination of the roots of $f(x)$ chosen (for example, the dihedral group of order 8 for our resolvent cubic). It should be observed, however, that the degree of the resolvent polynomials constructed, unlike the situation of the resolvent cubic for quartic polynomials, are in general much larger than the degree of $f(x)$. The effectiveness of this computational technique also depends heavily on the explicit knowledge of the possible transitive subgroups of S_n. For $n = 2, 3, \ldots, 8$ the number of isomorphism classes of transitive subgroups of S_n is 1, 2, 5, 5, 16, 7, 50, respectively. There is a great deal of interest in the computation of Galois groups, motivated in part by the problem of determining which groups occur as Galois groups over $\mathbb{Q}$.

We illustrate these techniques with some easier examples (from *The Computation of Galois Groups*, L. Soicher, Master's Thesis, Concordia University, Montreal, 1981).

Examples

(1) There are 5 isomorphism classes of transitive subgroups of S_5 given by the groups Z_5, D_{10}, F_{20}, the so-called Frobenius group of order 20 (the Galois group of $x^5 - 2$ with generators (1 2 3 4 5) and (2 3 5 4) in S_5), A_5 and S_5. The cycle type distributions for these groups are as follows:

cycle type :	1	2	(2, 2)	3	(2, 3)	4	5
Z_5	1						4
D_{10}	1		5				4
F_{20}	1		5			10	4
A_5	1		15	20			24
S_5	1	10	15	20	20	30	24.

Given this information, the irreducibility of $x^5 - x - 1$ (giving the transitivity on the 5 roots) and the cycle type (2,3) immediately shows that the Galois group of $x^5 - x - 1$ is S_5.

Consider now the polynomial $x^5 + 15x + 12$. The discriminant is $2^{10}3^45^5$ so the Galois group is not contained in A_5. There are two possibilities: S_5 or F_{20}. One can easily determine which is more likely by factoring the polynomial modulo a number of small primes and comparing the distribution of cycle types with those in the table above. This does not *prove* the probable Galois group is actually correct. To decide which of S_5 and F_{20} is correct one can compute the resolvent polynomial $R(x)$ of degree 15 whose roots are the distinct permutations under S_5 of $(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2$ for 4 of the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of $f(x)$. By definition, S_5 is transitive on the roots of $R(x)$ and it is not difficult to check using the explicit generators for F_{20} given above that F_{20} is not transitive on these 15 values. It follows that $R(x)$ will be a reducible polynomial over $\mathbb{Q}$ if and only if the Galois group of the quintic is F_{20}. One finds that for $x^5 + 15x + 12$ the resolvent polynomial $R(x)$ factors into a polynomial of degree 5 and a polynomial of degree 10, hence the Galois group for this quintic is F_{20}. One

can also use Exercise 21 of the previous section (cf. Exercise 6), which is also based on the computation of a related resolvent polynomial.

(2) Consider the polynomial $x^7 - 14x^5 + 56x^3 - 56x + 22$. The discriminant is computed to be $2^6 7^{10}$ so the Galois group is contained in A_7.

Factoring the polynomial for the 42 primes not equal to 7 between 3 and 193 gives a cycle type distribution of 1 1-cycle (2.38 %), 30 (3,3)-cycles (71.43 %), 11 7-cycles (26.19 %). There are 7 isomorphism classes of transitive subgroups of S_7, 4 of them contained in A_7. Of these, one contains no (3,3)-cycles, which leaves the three possibilities A_7, $GL_3(\mathbb{F}_2)$, or F_{21}, the Frobenius group of order 21 (which has generators (1 2 3 4 5 6 7) and (2 3 5)(4 7 6) in S_7). The cycle type distributions for these three are as follows:

cycle type:	1	2	(2, 2)	3	(2, 2, 3)	(3, 3)	(2, 4)	5	7
F_{21}	1					14			6
$GL_3(\mathbb{F}_2)$	1		21			56	42		48
A_7	1	21	105	70	210	280	630	504	720

It follows that there is a strong probability that the Galois group of this polynomial is the Frobenius group of order 21. This is actually the case (the verification requires computation of a resolvent of degree 35 and factoring it over $\mathbb{Z}$ — there are three factors, of degrees 7,7, and 21).

EXERCISES

1. Let p be a prime. Prove that the polynomial $x^4 + 1$ splits mod p either into two irreducible quadratics or into 4 linear factors using Corollary 41 together with the knowledge that the Galois group of this polynomial is the Klein 4-group.
2. (Cf. Exercise 48 of Section 6).
   (a) Let K be the splitting field of $x^6 - 2x^3 - 2$. Prove that if $[K : \mathbb{Q}] = 12$ then $K = \mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$ and K is generated over the biquadratic field $F = \mathbb{Q}(i, \sqrt{3})$ by $\alpha = \sqrt[3]{1 + \sqrt{3}}$ and by $\beta = \sqrt[3]{1 - \sqrt{3}}$. Show that if this is the case then the elements of order 3 in $\mathrm{Gal}(K/\mathbb{Q})$ lie in $\mathrm{Gal}(K/F)$. Conclude that any element of $\mathrm{Gal}(K/\mathbb{Q})$ of order 3 maps α to another cube root of $1 + \sqrt{3}$ and maps β to another cube root of $1 - \sqrt{3}$ and if it is the identity on α or β then it is the identity on all of K.
   (b) Show that the factorization of $f(x)$ into irreducibles over $\mathbb{F}_{13}$ is the polynomial $(x - 7)(x - 8)(x - 11)(x^3 + 3)$ and use Corollary 41 to show that $[K : \mathbb{Q}] = 36$.
   (c) Knowing that $G = \mathrm{Gal}(K/\mathbb{Q})$ is of order 36 determine all the elements of G explicitly and in particular show that G is isomorphic to $S_3 \times S_3$.
3. Prove that the Galois group of $x^5 + 20x + 16$ is A_5.
4. Prove that the Galois group of $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ is cyclic of order 5. [Show this is the minimal polynomial of $\zeta_{11} + \zeta_{11}^{-1}$.]
5. Prove that the Galois group of $x^5 + 11x + 44$ is the dihedral group D_{10} (cf. Exercise 21 of Section 7).
6. Prove that the Galois group of $x^5 + 15x + 12$ is F_{20}, the Frobenius group of order 20 (cf. Exercise 21 of Section 7).
7. Prove that the Galois group of $x^6 + 24x - 20$ is A_6.
8. Prove that the Galois group of $x^7 + 7x^4 + 14x + 3$ is A_7.

9. Determine a polynomial of degree 7 whose Galois group is cyclic of order 7.
10. Determine the probable Galois group of $x^7 - 7x + 3$.

14.9 TRANSCENDENTAL EXTENSIONS, INSEPARABLE EXTENSIONS, INFINITE GALOIS GROUPS

This section collects some results on arbitrary extensions E/F. These results supplement those of the preceding sections and complete the basic picture of how an arbitrary (possibly infinite) extension decomposes. Since this section is primarily intended as a survey, none of the proofs are included; whenever these proofs can be easily supplied by the reader we indicate this either in the text or (with hints) in the exercises.

Throughout this section E/F is an extension of fields. Recall that an element of E which is not algebraic over F is called transcendental over F. Keep in mind that extensions involving transcendentals are always of infinite degree. We generally reserve the expression "t is an 'indeterminate' over F", when we are thinking of evaluating t. Field theoretically, however, the terms transcendental and indeterminate are synonymous (so that the subfield $\mathbb{Q}(\pi)$ of $\mathbb{R}$ and the field $\mathbb{Q}(t)$ are isomorphic).

Definition.

(1) A subset $\{a_1, a_2, \ldots, a_n\}$ of E is called *algebraically independent* over F if there is no nonzero polynomial $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ such that $f(a_1, a_2, \ldots, a_n) = 0$. An arbitrary subset S of E is called *algebraically independent* over F if every finite subset of S is algebraically independent. The elements of S are called *independent transcendentals* over F.

(2) A *transcendence base* for E/F is a maximal subset (with respect to inclusion) of E which is algebraically independent over F.

Note that if E/F is algebraic, the empty set is the only algebraically independent subset of E. In particular, elements of an algebraically independent set are necessarily transcendental. Moreover, one easily checks that $S \subseteq E$ is an algebraically independent set over F if and only if each $s \in S$ is transcendental over $F(S - \{s\})$. It is also an easy exercise to see that S is a transcendence base for E/F if and only if S is a set of algebraically independent transcendentals over F and E is algebraic over $F(S)$.

Theorem. The extension E/F has a transcendence base and any two transcendence bases of E/F have the same cardinality.

Proof: The first statement is a standard Zorn's Lemma argument. The proof of the second uses the same "Replacement Lemma" idea as was used to prove that any two bases of a vector space have the same cardinality.

Definition. The cardinality of a transcendence base for E/F is called the *transcendence degree* of E/F.

Algebraic extensions are precisely the extensions of transcendence degree 0.