16 Algebra

16.1 The Galois Group of a Polynomial (7 units)

This project is related to material in the Part II course Galois Theory.

1 Introduction

The *Galois group* $G(f)$ of a polynomial f defined over a field K is the group of K-automorphisms of the field generated over K by the roots of f (the Galois group of the splitting field for f over K).

We shall consider Galois groups over the rationals and polynomials f which are monic and have coefficients in $\mathbb{Z}$. Assume that f has no repeated factor. Let f have degree $\partial f = n$ with Galois group a subgroup of the symmetric group S_n acting on the roots of f. The *decomposition group of f modulo p* is the Galois group $G_p(f)$ of f regarded as a polynomial over the finite field $\mathrm{GF}(p)$, provided that f modulo p does not have a repeated factor. The key result we shall use is that the decomposition group (when defined) is always cyclic and isomorphic to a subgroup of the Galois group of f. Furthermore, it is isomorphic in a way which preserves cycle types, so the cycle type of the generator of the decomposition group will also occur in the Galois group.

We shall use the decomposition groups to derive information about the Galois group of a polynomial f. For example, if $G(f)$ contains a 2-cycle, a $(n-1)$-cycle and an n-cycle, then it must be S_n. As the decomposition group is always cyclic, this information does not distinguish between groups with the same abelian subgroups, but computing a sufficient number of decomposition groups will usually determine the cyclic subgroups and hence often determine $G(f)$, although there is always the possibility that our answer will be too small if we do not compute enough.

2 The algorithms

To find the decomposition group of f modulo p, we need information about the factorisation of f over $\mathrm{GF}(p)$. There is a repeated factor in f iff f has a factor in common with its formal derivative f' and this can be determined by applying the Euclidean algorithm. Since $\mathrm{GF}(p^r)$ is the splitting field of any irreducible polynomial of degree r over $\mathrm{GF}(p)$ and the Galois group of $\mathrm{GF}(p^r)$ over $\mathrm{GF}(p)$ is the cyclic group C_r generated by $x \mapsto x^p$, it is only necessary to find the degrees of the irreducible factors in f in order to find its Galois group over $\mathrm{GF}(p)$. We let f_r be the product of all the irreducible factors of degree r in f: then there are $n_r = \partial f_r / r$ factors of degree r in f and the Galois group $G_p(f)$ of f over $\mathrm{GF}(p)$ is cyclic, where the generator has n_r r-cycles for each r.

We determine f_r by the observation that the elements of $\mathrm{GF}(p^r)$ all satisfy the equation $\phi_r(X) = X^{p^r} - X = 0$ and hence, if we proceed by successively removing the factors $f_1, \ldots, f_{r-1}$ then at the r^{th} stage we can obtain f_r by taking the highest common factor of the residue with ϕ_r.

> **Question 1** Write procedures to compute the quotient and remainder from dividing two polynomials over $\mathrm{GF}(p)$ and use them to write a procedure to find the highest common factor of two polynomials over $\mathrm{GF}(p)$. Include in your report some test output from all three procedures. Describe an efficient way of using your procedures to compute a large power of one polynomial modulo another polynomial.

Question 2 Write a procedure to compute the decomposition group of f modulo p. You should check first that the group is defined, that is, that f and f' have no common factor, and then decompose f into factors f_r. You should try to make this procedure reasonably efficient computationally. Use your procedures in a program that will read in a monic polynomial f with integer coefficients, and print out its decomposition groups for p up to, say, 97.

Question 3 Run your program for the polynomials

$$
\begin{aligned}
&X^2 + X + 41,\\
&X^3 + 2X + 1,\\
&X^3 + X^2 - 2X - 1,\\
&X^4 - 2X^2 + 4,\\
&X^4 - X^3 - 4X + 16,\\
&X^4 - 2X^3 + 5X + 5,\\
&X^4 + 7X^2 + 6X + 7,\\
&X^4 + 3X^3 - 6X^2 - 9X + 7,\\
&X^5 + 36,\\
&X^5 - 5X + 3,\\
&X^5 + X^3 - 3X^2 + 3,\\
&X^5 - 11X^3 + 22X - 11,\\
&X^6 + X + 1,\\
&X^7 - 2X^6 + 2X + 2,\\
&X^7 + X^4 - 2X^2 + 8X + 4,\\
&X^7 + X^5 - 4X^4 - X^3 + 5X + 1.
\end{aligned}
$$

Your program should tabulate its output in columns, so that the results for this question take only a few pages in total.

Question 4 Discuss the Galois groups of these polynomials in the light of your output, with special reference to the reducible polynomials. Assuming, in each case, that the group is the smallest possible, formulate a conjecture as to the relative frequencies of the various cycle shapes for a fixed polynomial f as p varies. Do any of the polynomials (especially those of smaller degree) appear to contradict this conjecture? If so, run your programs for these polynomials for higher values of p and see if this rectifies the matter.

Programming note

If you use MATLAB then you may wish to use the `DocPolynom` class that is included as an example in the help browser. To use this you should create a directory `@DocPolynom` and place `DocPolynom.m` into it. This will enable you to define and display (non-zero) polynomials and to carry out standard algebraic manipulations with them. There is no need to include the class file in your program listings (assuming you do not modify it). *[The latest version requires MATLAB 2022b or later to run.]*

If you use a computer algebra package (such as MAPLE), then you may find that some of the routines asked for in this project are included in the package. In such cases, no credit will be given for using the packaged routines — you are expected to write your own programs. You may wish to compare the answers given by your program and by the packaged routines.

References

[1] B. L. van der Waerden, *Modern Algebra vol. 1*

