Groups and Polynomials

Geoff C Smith
School of Mathematical Sciences
University of Bath
Claverton Down
Bath
Avon BA2 7AY ENGLAND

Introduction

In this tutorial lecture we will address ourselves to the subject of Galois Theory. This is a substantial area of modern algebra, and in the course of a single lecture, it is impossible to give the subject any more than a distant overview. The lecture will conclude with some remarks about possible applications of Galois Theory to Computer Algebra. As many of you will know, Evariste Galois (1811-1832) led a short and rather unhappy life. The tense political situation in France affected his career, such as it was, adversely. He even spent several months in gaol in consequence of his political activities. He died as a result of wounds received in a duel. It is clear that the pretext for the fatal conflict was "a woman"; it does not seem likely that the conflict was actually a consequence of the intense republican versus royalist rivalry in which he was deeply involved. This is not a talk about the life and times of Galois, though that would be a fascinating topic. He is, of course, in some ways a romantic figure; when one combines the dramatic events of his life with the difficulty he had in achieving recognition before his death, it is not surprising that the man is still a figure of considerable interest. However, his true significance is his fole in initiating modern algebra.

His early death is to be regretted — to put it mildly. One is reminded of the Chinese benediction

"May you live in uninteresting times" [ff]

The modern casting of the theory is very different from the times when Galois was writing. The very notion of a Group is due to Galois, and the language of modern mathematics had not yet been formulated. The works of Galois were not published until well after his death — in 1846 by Liouville [G]. The theory was subsequently advanced by the work of C Jordan [J]. The more concrete ways of thinking mathematically prevalent in those days may have some considerable appeal to this particular audience, so I commend to you especially the excellent text by Edwards [E], where he develops the theory in a constructive fashion. There are presumably texts in other languages which do a similar job. The Russian text by Postkinov [Po] presumably fills this niche in its untranslated form. Perhaps there is a more recent work which does the job as well. It is of course perfectly obvious that this talk is no substitute for a proper study of the theory, and some standard texts are included in the references [A], [E], [Po], [S].

Theory

The following theorem is known to well educated schoolchildren. We are so familiar with it that perhaps, in mature reflection, we do not give it the respect that it deserves. We shall prove it very carefully, in a manner which will generalize.

Theorem: If $F(X)$ is a polynomial in the variable X and has coefficients which are real numbers, then non-real roots of F occur in (complex conjugate) pairs.

It follows easily from results in elementary analysis, and the Fundamental Theorem of Algebra, that the number of non-real roots of $F(X)$ (counting multiplicities) is even. One simply distinguishes two cases depending on the parity of the degree of F. This however is a bad proof (not wrong, but bad). The more insightful proof runs as follows:

Let $g : \mathbf{C} \to \mathbf{C}$ denote complex conjugation, so $g(x + iy) = x - iy$.

One checks that g defines a field automorphism of $\mathbf{C}$, that is to say: For all complex numbers w and z, we have $g(w + z) = g(w) + g(z)$ and $g(wz) = g(w)g(z)$, and moreover $g(1) = 1$, so g is certainly a field monomorphism (1-1 and structure preserving). One notices also that g composed with itself is the identity map, so g is a bijection, and so g is indeed an automorphism of $\mathbf{C}$, the complex numbers. What complex numbers are fixed by g? Clearly $\mathbf{R}$, the set of real numbers. The fact that this fixed set is itself a field is no accident — we will return to this issue later.

Suppose that α is any complex root of F, so $F(\alpha) = 0$. This is an equation in $\mathbf{C}$, so we may apply the automorphism g to both sides. Write

$$F(X) = f_0 + f_1 X^1 + \ldots\ldots + f_n X^n \quad \text{(and each } f_i \text{ is real)}$$

so

$$F(\alpha) = f_0 + f_1 \alpha^1 + \ldots\ldots + f_n \alpha^n = 0$$

and therefore

$$g(F(\alpha)) = g(f_0) + g(f_1) g(\alpha)^1 + \ldots\ldots g(f_n) g(\alpha)^n = g(0)$$

since g is a field automorphism of the complex numbers. However, each f_i is actually real, so is fixed by g. The previous equation actually says:

$$f_0 + f_1 g(\alpha)^1 + \ldots\ldots + f_n g(\alpha)^n = F(g(\alpha)) = 0.$$

Thus if α is a root of F, then so is $g(\alpha)$. It might be tempting to conclude that the proof were finished, since when α is not real then α and $g(\alpha)$ are distinct and are interchanged by g. In fact there is a little more to say; we must allow for the possibility of multiple roots. We deal with this as follows; $\alpha + g(\alpha)$ and $\alpha g(\alpha)$ are both real (being fixed by g) so the polynomial