BULL. AUSTRAL. MATH. SOC. 12E05, 12F05
VOL. 57 (1998) [363–365]

CENTRALISERS OF GALOIS GROUP ACTIONS

MARK KISIN

If f is a polynomial over a field E, and σ a permutation of the roots of f, we show that σ is given by a polynomial p with coefficients in E (that is, $p(a) = \sigma(a)$ for each root a of f) if and only if σ commutes with all the Galois automorphisms.

If E is a field, and $\overline{E}$ a separable closure of E, then $\mathrm{Gal}\left(\overline{E}/E\right)$ acts on the roots of unity in $\overline{E}$ via the cyclotomic character. In particular the action of each Galois automorphism on roots of unity is a polynomial function. The purpose of this note is to point out that this is quite a general phenomenum. Namely we give two proofs of the following

THEOREM. *Let E be a field, $f \in E[X]$, a polynomial with distinct roots, and σ a permutation of the roots of f. There is a polynomial $p \in E[X]$ such that $p(a) = \sigma(a)$ for each root a of f if and only if σ commutes with the Galois action on the roots of f.*

In particular, if the roots of f generate an Abelian extension of E then the Galois action on the roots is given by polynomials in the sense above.

The theorem is pretty but not deep, and both proofs are completely elementary.

FIRST PROOF: We denote by G the absolute Galois group of E. The "only if" part is clear, since then for each $s \in G$ and root a of f we must have

$$s\big(\sigma(a)\big) = s\big(p(a)\big) = p\big(s(a)\big) = \sigma(s(a)).$$

Now suppose that σ commutes with the Galois action on the roots. If $f = f_1 f_2$ factors over E, then f_1 and f_2 are coprime. If $p_1, p_2 \in E[X]$ are such that $p_1(a) = \sigma(a)$, $p_2(b) = \sigma(b)$ for each root a of f_1 and b of f_2 then we may choose p congruent to p_1 modulo f_1 and p_2 modulo f_2.

Thus we may assume f is irreducible. Let a be a root of f, and $s \in G$. If $s(a) = a$ then $s\big(\sigma(a)\big) = \sigma\big(s(a)\big) = \sigma(a)$. So s fixes $\sigma(a)$ and $\sigma(a) \in E[a]$. Thus $\sigma(a) = p(a)$ for some $p \in E[X]$. If b is another root of f, then $b = t(a)$ for some $t \in G$, since f is

Received 20th August, 1997

irreducible. Hence $\sigma(b) = \sigma\big(t(a)\big) = t\big(\sigma(a)\big) = t\big(p(a)\big) = p\big(t(a)\big) = p(b)$, and p is the required polynomial. □

SECOND PROOF: We retain the notation above, and give a second proof of the "if" part.

Let $a_1, \dots, a_n$ be the roots of f, and denote by f_i $(1 \leqslant i \leqslant n)$ the polynomial $f(X)/(X - a_i)$. We set

$$p(X) = \sum_{i=1}^{n} [f_i(X)/f_i(a_i)]\sigma(a_i).$$

This is the Lagrange interpolation formula, and we have $p(a_i) = \sigma(a_i)$ for each i.

To see that $p \in E[X]$ we extend the action of G to $E[a_1, \dots, a_n][X]$ by letting G act on the coefficients of polynomials. If $s \in G$, choose $w \in S_n$ such that $s(a_i) = a_{w(i)}$. We get

$$\begin{aligned} s\big(p(X)\big) &= \sum_{i=1}^{n} \big[f_{w(i)}(X)/f_{w(i)}\big(a_{w(i)}\big)\big] s\big(\sigma(a_i)\big) = \sum_{i=1}^{n} \big[f_{w(i)}(X)/f_{w(i)}\big(a_{w(i)}\big)\big] \sigma\big(s(a_i)\big) \\ &= \sum_{i=1}^{n} \big[f_{w(i)}(X)/f_{w(i)}\big(a_{w(i)}\big)\big] \sigma\big(a_{w(i)}\big) = p(X). \end{aligned}$$

□

An amusing application of the above theorem is a proof of the following theorem on permutation groups [**1**, Theorem 4.2A].

COROLLARY. *Let $H \subset S_n$ be a transitive permutation group. Then the only element of the centraliser of H in S_n which has a fixed point is the identity.*

In particular if H is Abelian it is its own centraliser.

PROOF: Let E and f be as in the theorem. Denote by J the group of permutations of the roots of f induced by G. Choose E and f so that J is isomorphic to H as a permutation group. This is possible, since one can choose E and f so that $J \xrightarrow{\sim} S_n$ and then replace E by a finite extension.

If $\sigma \in S_n$ commutes with all the elements of J then by the theorem we have $\sigma(a) = p(a)$ for some $p \in E[X]$ and each root a of f. If $\sigma(a) = a$ then we have $p(a) = a$. Since p can be chosen so that $\deg p < \deg f = n$, and f is irreducible, we see that $p(X) = X$ and $\sigma = \mathrm{id}$. □

Finally we pose the following question:

Suppose that E is a local field, and that we are given a sequence $f_1, f_2, \dots$ of polynomials in $E[X]$ with distinct roots and such that $f_i \mid f_{i+1}$ for each i. We let $\mathcal{R}$ denote the union of the roots of the f_i. If σ is an automorphism of $\mathcal{R}$, when is there a power series p with coefficients in E such that $p(a) = \sigma(a)$ for each $a \in \mathcal{R}$? In

particular the equality means that the left hand side is well defined. Clearly σ must commute with the Galois action on $\mathcal{R}$, but this is perhaps not sufficient because of convergence problems.

We remark that if $\mathcal{R}$ is the set of torsion points of a Lubin - Tate formal group over the ring of integers of E, (so the Galois action on $\mathcal{R}$ is Abelian) and σ is induced by a Galois automorphism, then the required p exists [**2,** Proposition 4.9]. The situation where $\mathcal{R}$ consists of elements of the form $\zeta - 1$ with ζ a p power root of unity is a special case, the power series associated to $\sigma \in G^{\mathrm{ab}}$ being $p(X) = (1+X)^{\omega(\sigma)} - 1$, where $\omega : G^{\mathrm{ab}} \longrightarrow \mathbb{Z}_p^*$ is the cyclotomic character.

References

[1] J. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163** (Springer-Verlag, Berlin, Heidelberg, New York, 1996).

[2] K. Iwasawa, *Local class field theory*, Oxford Mathematical Monographs (Oxford University Press, New York, 1986).

Department ofMathematics
University of Sydney
Sydney NSW 2006
Australia