Roots appear in quanta: exercise solutions

Alexander R. Perlis

Herein are solutions to the exercises given in [1]. Let K be a field, and $f(X) \in K[X]$ an irreducible polynomial. The *root quantum number* $r_K(f)$ is the number of roots of f in the stem field $K(\alpha)$, where α is an arbitrary choice of root of f. It was shown that $r_K(f)$ is well-defined and divides the degree of f.

We start by establishing the connection with Galois theory. Let f be irreducible and separable over K. Let L/K be the splitting field and G the Galois group. Fix a root α, and let $H \subset G$ be the subgroup fixing α. A root of f lies in $K(\alpha)$ if and only if it is fixed by H, so $r_K(f)$ equals the number of roots fixed by H. Any automorphism of $K(\alpha)/K$ is determined by the image of α, which must be another root of f lying in $K(\alpha)$; conversely, the map sending α to any root of f in $K(\alpha)$ gives rise to an automorphism. Thus $r_K(f)$ equals the cardinality of $\operatorname{Aut}\bigl(K(\alpha)/K\bigr)$. Finally, $r_K(f)$ equals the index $[\mathrm{N}_G(H) : H]$ of H in its normalizer, since Galois theory (see below) tells us $\operatorname{Aut}\bigl(K(\alpha)/K\bigr) \cong \mathrm{N}_G(H)/H$.

Proposition. *Let L/K be a finite Galois extension with Galois group G, let H be a subgroup, and let L^H be its fixed field. Then* $\operatorname{Aut}(L^H/K) \cong \mathrm{N}_G(H)/H$.

Proof. An element $g \in G$ restricts to an automorphism of L^H/K if and only if $g(L^H) \subseteq L^H$, and g is trivial on L^H precisely when $g \in H$. Any automorphism of L^H/K extends to an automorphism of L/K, so we must show: the $g \in G$ that induce automorphisms of L^H/K are precisely the $g \in \mathrm{N}_G(H)$. If $g \in \mathrm{N}_G(H)$ and $x \in L^H$, then $Hgx = gHx = gx$, so gx is fixed by H, whence $gx \in L^H$. If $g \notin \mathrm{N}_G(H)$, then there exists $h \in H$ so that $g^{-1}hg \notin H$, so there exists $x \in L^H$ with $g^{-1}hgx \neq x$, whence $hgx \neq gx$, so $gx \notin L^H$. □

The exercises concern triples (K, n, r) that indicate the existence of an irreducible polynomial $f(X)$ in $K[X]$ of degree n with $r_K(f) = r$. The necessary condition is that r must divide n.

Exercise 1. *Show that* $(\mathbf{Q}, 2, 1)$ *does not appear.*

Solution. For $(\mathbf{Q}, 2, 1)$ to appear, there would have to exist a quadratic irreducible polynomial over $\mathbf{Q}$, call its roots α and β, such that $\mathbf{Q}(\alpha)$ contains precisely one root of f: either $\beta = \alpha$ or $\beta \notin \mathbf{Q}(\alpha)$. But irreducible polynomials over $\mathbf{Q}$ have distinct roots, ruling out $\beta = \alpha$, and over $\mathbf{Q}(\alpha)$ the factorization of f must have the form $f(X) = a(X - \alpha)(X - \beta)$, whence $\beta \in \mathbf{Q}(\alpha)$. □

Remark. The precise class of fields K for which $(K, 2, 1)$ does not appear comprises the fields that admit no quadratic irreducible polynomial with a repeated root. This class includes all perfect fields, and thus includes all finite fields and all fields of characteristic 0.

Exercise 2. *Find a field K for which $(K, 2, 1)$ does appear.*

Solution. Let $K = \mathbf{F}_2(t)$, the field of rational expressions in t with coefficients in the finite field $\mathbf{F}_2$. The polynomial $X^2 - t$ is quadratic and irreducible, but not separable: its factorization over $K(\sqrt{t})$ is $(X - \sqrt{t})^2$. Although $K(\sqrt{t})$ contains all roots of f, there is only one root. □

Remark. The reader may feel that roots ought to be counted with multiplicity. To that end, define $\ell_K(f)$ to be the number of linear factors in the factorization of f over any stem field, and call $\ell_K(f)$ the *linear factor quantum number* of f. Letting $s_K(f)$ be the number of stem fields, we have:

$$r_K(f) \cdot s_K(f) = \operatorname{Sep}\operatorname{Deg}(f), \qquad \ell_K(f) \cdot s_K(f) = \operatorname{Deg}(f).$$

If we were to consider triples (K, n, ℓ) instead of (K, n, r), then the triple $(K, 2, 1)$ would *never* occur, no matter what field K was chosen.

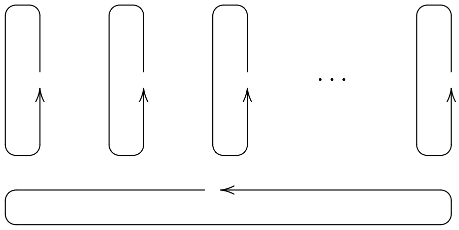
Exercise 3. *Let r divide n. Show that there exists K for which (K, n, r) appears.*

Solution. The existence of a $(K, 2, 1)$ was established in the solution to the previous exercise, so we now assume $(n, r) \neq (2, 1)$. Hilbert showed: for each n, there exists $f(X) \in \mathbf{Q}[X]$ of degree n with Galois group S_n. If $r = 1$, then we're done: a stem field of f over $\mathbf{Q}$ will contain precisely one root of f. (Here we used the assumption $(n, r) \neq (2, 1)$.) Henceforth we assume $r > 1$.

We will be done if we can produce a field K and an irreducible separable polynomial $f(X) \in K[X]$ of degree n whose Galois group has the property that a point stabilizer fixes precisely r points. We start with $f(X) \in \mathbf{Q}[X]$ with Galois group S_n, as in the previous paragraph. To produce K, we first cook up a subgroup $G \subset S_n$ with the desired properties: it must be transitive on n points, and a point stabilizer must fix precisely r points. For example, label the roots of f in vertical packets of size r:

$$\begin{array}{ccccc}
\alpha_{11}, & \alpha_{21}, & \alpha_{31} & & \alpha_{(n/r)1}, \\
\alpha_{12}, & \alpha_{22}, & \alpha_{32} & \cdots & \alpha_{(n/r)2}, \\
\vdots & \vdots & \vdots & & \vdots \\
\alpha_{1r}, & \alpha_{2r}, & \alpha_{3r} & & \alpha_{(n/r)r}.
\end{array}$$

Let G be the group of permutations on these n roots generated by independent cyclic permutations on each vertical packet, together with a cyclic permutation on the overall set of packets. This construction is called a *wreath product.*



If some group element $g \in G$ fixes one root in a vertical packet, then g ties down the vertical cycle of that packet as well as the overall horizontal cycle, but the remaining vertical cycles remain free and independent. In other words, all roots in one packet are fixed, but no roots in other packets are fixed. (Here we used the assumption $r > 1$. Otherwise all roots would be fixed.)

Letting $L/\mathbf{Q}$ be the splitting field of f, let $K = L^G$ be the fixed field of the group G constructed above. Then L/K is Galois with G as Galois group. This group permutes the roots of f transitively, so $f(X)$ remains irreducible when viewed as a polynomial in $K[X]$. By construction, if α is any root of f in L, then the stem field $K(\alpha)$ contains precisely r roots of f, so $r_K(f) = r$. In other words, we have produced a (K, n, r). □

Exercise 4. *Let r divide n. Except for $(\mathbf{Q}, 2, 1)$, show that $(\mathbf{Q}, n, r)$ appears.*

Solution. The trick here is to modify the solution to the previous exercise to obtain the base field $\mathbf{Q}$. Since we already showed that $(\mathbf{Q}, n, 1)$ appears when $n \neq 2$, we henceforth assume $r > 1$. Recall that we constructed a wreath product $G \subset S_n$ and showed it to occur as the Galois group of an irreducible polynomial with coefficients in a field K, thus giving us a (K, n, r). Now we will show that the same group occurs as the Galois group of an irreducible polynomial with coefficients in $\mathbf{Q}$, thus giving us a $(\mathbf{Q}, n, r)$. To do this, we will show that G is solvable and then appeal to a theorem of Shafarevich.

The wreath product construction of G has the explicit description of a semidirect product

$$G = (\underbrace{C_r \times C_r \times \cdots \times C_r}_{n/r \text{ copies}}) \rtimes C_{n/r},$$

where the symbols denote cyclic groups of the indicated order, and the action of $C_{n/r}$ is to permute the factors on the left. The chain

$$1 \subset C_r \subset C_r \times C_r \subset \cdots \subset (C_r \times C_r \times \cdots \times C_r) \subset G$$

has cyclic quotients, so G is solvable. Now apply the following theorem. □

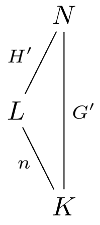
Theorem (Shafarevich). *If G is a finite solvable group, then there exists a finite Galois extension of $\mathbf{Q}$ with Galois group isomorphic to G.*

Proof. See [2, Thm 9.5.1]. □

Actually, for our purposes, we need the more precise statement: *If G is a solvable transitive subgroup of S_n, then there exists an irreducible polynomial $f(X) \in \mathbf{Q}[X]$ of degree n and a labeling of the roots so that G is the root permutation group of f.* The point is that we have a particular permutation representation of G in mind, namely the wreath product from earlier, and knowing merely that G occurs *somehow* as a Galois group does not trivially imply that it occurs in the form of our wreath product. (After all, S_3 also occurs in its left regular representation as a transitive subgroup of S_6, so knowing merely that S_3 occurs as a Galois group does not immediately tell us that it occurs as the root permutation group of a degree 6 polynomial. For a more elaborate example, S_7 admits non-conjugate copies of $\mathrm{GL}(3,\mathbf{F}_2)$ as subgroups, so when $\mathrm{GL}(3,\mathbf{F}_2)$ occurs as a Galois group of a degree 7 polynomial, which of the possible root permutation groups do we get? In fact, in both examples, all representations occur.) As we show below, every faithful transitive permutation representation of an abstract Galois group occurs concretely as the root permutation group of a polynomial. This gives us the precise form of Shafarevich's theorem and completes the exercise solution.

Proposition. *Let G be a given transitive subgroup of S_n for some n. If there exists a finite Galois extension of a field K with Galois group abstractly isomorphic to G, then there exists an irreducible polynomial $f(X) \in K[X]$ of degree n and a labeling of the roots so that the Galois group of f, viewed as a root permutation group, is precisely G.*

Proof. Let $H \subseteq G$ be the stabilizer of the symbol 1; then there is a canonical labeling of the n cosets in G/H so that G acts on G/H exactly the same way G acts on the original n symbols. In particular, the action of G on G/H is faithful and transitive. Now suppose that G is abstractly isomorphic to the group $G' = \mathrm{Aut}(N/K)$ for some finite Galois extension N of K. Under that isomorphism, H corresponds to a subgroup $H' \subseteq G'$. Let L be the subfield of N fixed by H'. Then G' acts faithfully and transitively on G'/H' exactly the same way that G acts on G/H. In particular, one can easily check that N is the normal closure of L/K, since the normal closure of L/K in N is the subfield of N corresponding to the intersection of the conjugates of H' in G', and that intersection is 1 since the action is faithful. Now write $L = K(\theta)$. Then θ is a root of an irreducible polynomial $f(X) \in K[X]$ of degree n. You can identify the n roots of $f(X)$ with the n cosets in G'/H'. We have produced an irreducible polynomial whose Galois group G' acts on the n roots exactly like G acts on the original n objects. □



ACKNOWLEDGMENTS. I thank Robert Perlis for the argument in the final proposition and for helping to improve earlier versions of this note. I thank Klaux Lux for the example of non-conjugate yet isomorphic subgroups of S_7.

REFERENCES

[1] Alexander Perlis, *Roots Appear in Quanta*, Amer. Math. Monthly **111** (2004), 61–63.

[2] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000, ISBN 3-540-66671-0. MR 2000j:11168

Department of Mathematics
The University of Arizona
Tucson, Arizona 85721–0089
aprl@math.arizona.edu