

Classroom



In this section of Resonance, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. “Classroom” is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Rajat Tandon
Department of Mathematics
and Statistics
University of Hyderabad
Hyderabad 500 046, India.
Email: rtsm@uohyd.ernet.in

Roots are not Contained in Cyclotomic Fields

The square root of any integer is contained in a cyclotomic field i.e. an extension field $\mathbb{Q}(\zeta_n)$ of \mathbb{Q} generated by $\zeta_n = e^{\frac{2\pi i}{n}}$. There is a famous theorem of Kronecker and Weber (see the remarks at the end) which vastly generalises this fact. In what follows, if $\alpha_1, \alpha_2, \dots, \alpha_n$ are complex numbers, we denote by $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ the smallest subfield of \mathbb{C} containing the α_i 's. As in the case of Fermat's last theorem (FLT, where $x^n + y^n = z^n$ has integer solutions only in the case $n=2$) the surprising fact is that other n th roots (other than square roots) are never contained in a cyclotomic extension. Of course, one must exercise a little care. For instance $\sqrt[4]{4} = \sqrt{2}$ is a square root and hence contained in a cyclotomic extension. The point here is that $\sqrt[4]{4}$ is not a genuine fourth root; it is, in fact, a square root.

Definition 1. *If a is an integer greater than 1 then the real number $\sqrt[n]{a}$ is said to be a genuine n th root if it cannot be written in the form $\sqrt[m]{b}$ for some integer b and some $m < n$.*

In particular, a genuine n th root for $n > 1$ is irrational for, if it is rational, then it is of the form $\sqrt[m]{b}$ for some



integer b . We have the following theorem:

Theorem 2. *Let a be any integer. Then, \sqrt{a} is contained in a cyclotomic field. If $\sqrt[n]{a}$ is a genuine n th root where a is an integer greater than 1 and n an integer greater than 2, then $\sqrt[n]{a}$ is not contained in any cyclotomic field.*

The first assertion is very well-known and is easy to establish. While proving it, one actually proves a stronger statement viz.,

Proposition 3. *If p is a prime, then $\sqrt{(-1)^{(p-1)/2}p} \in \mathbb{Q}(\zeta_p)$.*

Observe that if $\sqrt[n]{a}$ is genuine and $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ is the factorisation of a into distinct prime powers then $\text{g.c.d.}(e_1, e_2, \dots, e_r, n) = 1$. For, if $t = (e_1, e_2, \dots, e_r, n)$ and $b = p_1^{e_1/t} p_2^{e_2/t} \dots p_r^{e_r/t}$ then $\sqrt[n]{a} = \sqrt[t]{b}$. If then n has an odd prime factor p , in order to show that $\sqrt[n]{a}$ is not contained in any cyclotomic extension it suffices to show that $(\sqrt[n]{a})^{n/p} = \sqrt[p]{a}$ is not contained in a cyclotomic extension. On the other hand, if $n = 2^r$, $r \geq 2$ it suffices to show that $(\sqrt[n]{a})^{n/4} = \sqrt[4]{a}$ is not contained in any cyclotomic extension i.e., it suffices (as in the case of FLT) to prove our theorem for $n = 4$ or p where p is any odd prime.

The proof follows from the following propositions which can be found in any standard text on Galois theory (see, for instance [1]). We will also refer to the article [2] on Galois theory by B Sury which appeared in *Resonance*. In what follows K and F will always denote subfields of \mathbb{C} and if K is any such field we denote by $G(K)$ the group of automorphisms of K . $[K : F]$ denotes the dimension of K as a vector space over F .

Proposition 4. *If $F \subseteq K \subseteq L$ then $[L : F] =$*

$$[L : K][K : F].$$



It is easy to see that if α_i 's form a basis of K over F and β_j 's form a basis of L over K then the $\alpha_i\beta_j$'s form a basis of L over F .

Proposition 5. $[F(\alpha) : F]$ is equal to the degree of the unique monic polynomial f_α of minimal degree in $F[X]$ satisfied by α and this is the same as the degree of any irreducible polynomial in $F[X]$ satisfied by α .

(See lemma in [2].) It can easily be seen by using the Euclidean algorithm for polynomials that f_α divides any polynomial in $F[X]$ that has α as a root and hence divides any irreducible polynomial g satisfied by α . Irreducibility of g implies that $g = cf_\alpha$ for some constant c in F .

Proposition 6. The group $G(\mathbb{Q}(\zeta_m))$ of automorphisms of the field $\mathbb{Q}(\zeta_m)$ for any $m > 2$ is abelian; in fact, it is isomorphic to the group of units in the ring $\mathbb{Z}/m\mathbb{Z}$.

It is clear that if σ is an automorphism of $\mathbb{Q}(\zeta_m)$ then since $\zeta_m^m = 1$ we get $\sigma(\zeta_m)^m = 1$ so $\sigma(\zeta_m)$ is another m th root of 1. Since an automorphism of a group preserves order and σ is an automorphism of the multiplicative group $(\mathbb{Q}(\zeta_m) - \{0\})$, $\sigma(\zeta_m)$ has order m so $\sigma(\zeta_m) = \zeta_m^i$ for some i coprime to m . We thus have a map $\sigma \rightarrow i$ from $G(\mathbb{Q}(\zeta_m))$ to the group of units in $\mathbb{Z}/m\mathbb{Z}$. That the map is a homomorphism is a simple exercise. It is clear that σ is completely determined by its action on ζ_m since ζ_m generates $\mathbb{Q}(\zeta_m)$. Hence the map is injective. That the map is surjective follows from the proposition 8.

Proposition 7. If $\mathbb{Q} \subseteq F \subseteq K$ where F and K are each generated over \mathbb{Q} by the roots of some polynomials in $\mathbb{Q}[X]$ i.e. F and K are splitting fields of polynomials in $\mathbb{Q}[X]$ (see [2]) then $G(F)$ is isomorphic to $G(K)/G(K/F)$ where $G(K/F)$ denotes the subgroup of $G(K)$ consisting of those automorphisms of K which fix



the elements of F . Hence if $G(K)$ is abelian so also is $G(F)$.

This follows easily if we consider the restriction map from $G(K)$ to $G(F)$. The fact that if $\sigma \in G(K)$ then $\sigma(F) = F$ follows from the fact that F is normal over \mathbb{Q} (refer [2], Box 14). For, suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$, where the α_i 's are roots of some polynomial $f(x)$ in $\mathbb{Q}[X]$. Since $f(\alpha_i) = 0$, $\sigma(f(\alpha_i)) = 0$. But $\sigma(f(\alpha_i)) = f(\sigma(\alpha_i))$, so $\sigma(\alpha_i)$ must be another root of f i.e. $\sigma(\alpha_i) = \alpha_j$ for some j ; σ permutes the roots of f and so $\sigma(F) = F$.

Proposition 8. *If K is generated over F by the roots of some polynomial in $F[X]$ and α, α' are two roots in K of an irreducible polynomial in $F[X]$ then there exists an automorphism σ in $G(K/F)$ such that $\sigma(\alpha) = \alpha'$.*

We have an isomorphism (just the substitution map) from $\frac{F[X]}{(f)}$ to $F(\alpha)$ which maps $X + (f)$ to α and similarly an isomorphism from $\frac{F[X]}{(f)}$ to $F(\alpha')$ which maps $X + (f)$ to α' . Hence we have an isomorphism from $F(\alpha)$ to $F(\alpha')$ which maps α to α' . This map extends to an automorphism of K (see proposition 5.2 in [1]).

Proposition 9. *If p is an odd prime or 4 and if $\sqrt[p]{a}$ is genuine with $a > 1$ then $G(\sqrt[p]{a}, \zeta_p)$ is not abelian.*

If p is an odd prime $\mathbb{Q}(\zeta_p)$ is the field generated over \mathbb{Q} by the roots of $1 + X + X^2 + \dots + X^{p-1}$. If p is an odd prime or 4 and $a > 1$ then $\mathbb{Q}(\sqrt[p]{a}, \zeta_p)$ is the field generated over \mathbb{Q} by the roots of $X^p - a$. Both these polynomials are irreducible over \mathbb{Q} . Hence

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \begin{cases} p - 1 & \text{if } p \text{ is odd} \\ 2 & \text{if } p = 4 \end{cases}$$

and $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$. Hence by proposition 4

$$[\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}] = \begin{cases} p(p - 1) & \text{if } p \text{ is odd} \\ 8 & \text{if } p = 4. \end{cases}$$



It follows again by proposition 4 that $[\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}(\zeta_p)] = p$ and $[\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}(\sqrt[p]{a})] = p - 1$ or 2 according as p is odd or 4 , respectively. Hence by proposition 5, $X^p - a$ is irreducible over $\mathbb{Q}(\zeta_p)$ and $1 + X + X^2 + \dots + X^{p-1}$ is irreducible over $\mathbb{Q}(\sqrt[p]{a})$ if p is odd whilst $X^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt[4]{a})$. Observe that $\sqrt[p]{a}$ and $\sqrt[p]{a}\zeta_p$ are roots of $X^p - a$ and ζ_p and ζ_p^2 are roots of $1 + X + \dots + X^{p-1}$ if p is odd whereas ζ_p and ζ_p^3 are roots of $X^2 + 1$ if $p = 4$. Hence by proposition 8 there exists an automorphism $\sigma \in G(\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}(\zeta_p))$ (i.e. σ fixes ζ_p) such that $\sigma(\sqrt[p]{a}) = \sqrt[p]{a}\zeta_p$ and there exists a $\tau \in G(\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}(\sqrt[p]{a}))$ (i.e. τ fixes $\sqrt[p]{a}$) such that $\tau(\zeta_p) = \zeta_p^2$ if p is odd and $\tau(\zeta_p) = \zeta_p^3$ if $p = 4$. Hence $\sigma\tau(\sqrt[p]{a}) = \sigma(\sqrt[p]{a}) = \sqrt[p]{a}\zeta_p$ whereas

$$\tau\sigma(\sqrt[p]{a}) = \tau(\sqrt[p]{a}\zeta_p) = \tau(\sqrt[p]{a})\tau(\zeta_p) = \begin{cases} \sqrt[p]{a}\zeta_p^2 & \text{if } p \text{ is odd} \\ \sqrt[p]{a}\zeta_p^3 & \text{if } p = 4. \end{cases}$$

In either case $\sigma\tau \neq \tau\sigma$ and $G(\mathbb{Q}(\sqrt[p]{a}, \zeta_p))$ is not abelian.

Observe that if $\mathbb{Q}(\sqrt[n]{a}) \subseteq \mathbb{Q}(\zeta_m)$ then $\mathbb{Q}(\sqrt[n]{a}, \zeta_n) \subseteq \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$ where $[m, n]$ is the l.c.m. of m and n . If $\mathbb{Q}(\sqrt[p]{a}, \zeta_p)$ was contained in the cyclotomic extension $\mathbb{Q}(\zeta_m)$ its group of automorphisms would, by proposition 7, be the quotient of the abelian group $G(\mathbb{Q}(\zeta_m))$ and hence abelian.

Remarks

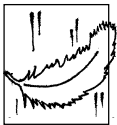
We have apparently proved the stronger result that for a genuine p -th root $\sqrt[p]{a}$ (with p an odd prime and $a > 1$), the Galois extension field generated by it is not an abelian extension of \mathbb{Q} . However, this is not really a stronger statement. The deep theorem of Kronecker and Weber referred to in the introduction says that any abelian extension of \mathbb{Q} is contained in a cyclotomic extension. The interesting question is whether one can similarly obtain the abelian extensions of any algebraic number field by adjoining special values of transcendental functions. For imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$,



this has been solved using the so-called theory of complex multiplication. Roughly, the role of the function $e^{2\pi ix}$ is taken by the elliptic modular j -function and the values are considered at points of finite order on elliptic curves (in place of the circle as was in the case of the Kronecker–Weber theorem). The general question is known as Kronecker’s ‘jugendtraum’ (the German word means ‘dream of youth’) and is still open. It is one of the famous ‘Hilbert problems’ (the 12th problem). Hilbert writes in his 1900 address at the International Congress of Mathematicians that the extension of Kronecker’s theorem to any algebraic number field seems to him to be of the greatest importance and that he regards this as one of the most profound and far-reaching problems in the theory of numbers.

Suggested Reading

- [1] M Artin, *Algebra*, Prentice-Hall of India, New Delhi, 1994.
 [2] B Sury, *The Theory of Equations and the Birth of Modern Group Theory*, *Resonance*, Vol 4, No. 10, 1999.



Churchill Eisenhart, son of the former dean of Princeton University’s Graduate School, tells how a telephone call was taken in the dean’s office shortly after Einstein’s arrival. “*May I speak with Dean Eisenhart, please?*” the speaker asked. On being told that the dean was out, the caller said: “*Perhaps you can tell me where Dr. Einstein lives*”. But it has been agreed that everything should be done to protect him from inquisitive callers, so the request was politely refused. “*The voice on the telephone dropped to a near whisper,*” writes Eisenhart, “and continued: ‘*Please do not tell anybody, but I am Dr Einstein. I am on my way home and have forgotten where my house is*’”.

From:
Einstein: The Life and Times by Ronald W Clark

