Casus irreducibilis

Author: David Yao

May 18, 2016

Abstract algebra

Theorem 0.1 (casus irreducibilis) If \( p(x) \in \mathbb{Q}[x] \) is an irreducible cubic polynomial with three real roots, then it is impossible to obtain any of the roots with only real radicals.

Lemma 0.2 Suppose \( F \) is a subfield of \( \mathbb{R} \) and let \( a \) be an element of \( F \). Let \( p \) be prime and let \( \alpha = \sqrt[p]{a} \) be the \( p \)th real root of \( a \). Then \( [F(\alpha) : F] = 1 \) or \( p \).

Proof of Lemma 0.2 Let \( m_\alpha \) be the minimal polynomial of \( \alpha \) over \( F \), and suppose its degree is \( d \leq p \). Since \( m_\alpha \) divides \( x^p - a \), all its roots are \( p \)th roots of \( a \), in the form of \( \alpha \zeta_p^j \) for some integer \( j \), where \( \zeta_p \) is the \( p \)th root of unity.

The constant term of \( m_\alpha \) lies in \( F \) and is the product of all its roots, so it is \( \alpha^d \zeta_p^k \) for some integer \( k \), as products of \( p \)th roots of unity is still a \( p \)th root of unity. Therefore \( \alpha^d \zeta_p^k \) is real. Since \( \alpha^d \) is real, \( \zeta_p^k \) is real, so \( \zeta_p^k = \pm 1 \).

Therefore \( \alpha^d \in F, \exists a, b \in \mathbb{Z} \) s.t. \( ad + bp = (d, p) \) by Euclid’s Algorithm. So \( \alpha^{(d, p)} = (\alpha^d)^a (\alpha^p)^b \in F \).

Proof of casus irreducibilis: Let \( p(x) \) be an irreducible polynomial in \( \mathbb{Q}[x] \) with three real roots \( a, b, c \). Consider the discriminant \( D \) of \( p(x) \).

\[
D = (a - b)^2(a - c)^2(b - c)^2
\]

Since we are in \( \mathbb{C} \), \( p(x) \) is separable and \( a, b, c \) are all distinct. Since they are all real, \( D > 0 \), and it has a real square root \( \sqrt{D} \in \mathbb{R} \). \( p(x) \) is still irreducible in \( Q(\sqrt{D}) \) because a quadratic extension cannot contain any root of \( p \), an irreducible cubic whose roots have degree 3 over \( Q \). Now, since \( D \) is a perfect square in \( Q(\sqrt{D}) \), the Galois group of \( p(x) \) over \( Q(\sqrt{D}) \) is inside \( A_3 \), so the splitting field of \( p(x) \) over \( Q(\sqrt{D}) \) is at most degree 3. In other words, adjoining any root to \( Q(\sqrt{D}) \) will give all three roots.

By way of contradiction, suppose one of the roots is expressible in real radicals, then it lives inside a real radical extension of \( Q \), and consequently lives inside a real radical extension of \( Q(\sqrt{D}) \). By the previous discussion, all three roots are in that real radical extension of \( Q(\sqrt{D}) \). We hence have the tower

\[
\mathbb{Q} = K_0 \subset K_1 = \mathbb{Q}(\sqrt{D}) \subset K_2 \subset \cdots \subset K_s
\]

where each \( K_i \subset \mathbb{R} \) and \( K_{i+1} = K_i(\sqrt{\alpha_i}) \) for some \( \alpha_i \in K_i \), and \( a, b, c \in K_s \).

Notice that \( s \geq 2 \) because \( p(x) \) is irreducible over \( K_1 \), per previous discussion.

Notice also that for a simple radical extension \( F(\sqrt[p]{\alpha})/F \), it can be further broken down into two simple radical extensions \( F(\sqrt[p]{\alpha})/F(\sqrt[p]{\alpha})/F \). Therefore WLOG, we can assume that \( K_{i+1} = K_i(\sqrt[p]{\alpha}) \) for some prime \( p_i \). By Lemma 0.2 we know that \( [K_{i+1} : K_i] = p_i \).

WLOG, suppose that \( s \) is chosen so that \( K_s \) is the first field in the tower to split \( p(x) \), then by previous discussion, \( K_{s-1} \) does not contain any of the roots \( a, b, c \).

Since \( K_{s-1} \) contains no root of \( p(x) \), \( p(x) \) is irreducible over \( K_{s-1} \). Since \( p(x) \) splits in \( K_s \), \([K_s : K_{s-1}] \) is a multiple of 3. However, this is a prime degree extension by assumption so \([K_s : K_{s-1}] = 3 = p_{s-1} \), i.e. \( K_s = K_{s-1}(a, b, c) \) is the splitting field of \( p(x) \) over \( K_{s-1} \), hence it is a Galois extension. By construction, \( K_s = K_{s-1}(\sqrt[p]{\alpha_{s-1}}) \), and \( x^3 - \alpha_{s-1} \) is irreducible over \( K_{s-1} \). As a Galois extension, \( K_s \) contains a real third root of \( \alpha_{s-1} \), call it \( \beta \). It must contain the other two third roots as well, namely \( \beta \zeta_3 \) and \( \beta \zeta_3^2 \). So \( \zeta_3 \in K_s \), which contradicts \( K_s \subset \mathbb{R} \).

References