MA3D5 Galois Theory

Daan Krammer

January 9, 2009

Contents

1 Symmetric functions

1.1 Reminders on rings

Rings. All our rings are commutative with one. Thus, a **ring** is a set A together with two specified elements $0 = 0_A \in A$, $1 = 1_A \in A$ and two binary operations $A \times A \to A$ written $(a,b) \mapsto a+b$ and $(a,b) \mapsto ab$ with the following properties, for all $a,b,c \in A$:

$$\begin{array}{ccccc} a+b=b+a, & & (a+b)+c=a+(b+c), & & a+0=a, \\ ab=ba, & & (ab)c=a(bc), & & a\cdot 1=a, \\ & & a(b+c)=ab+ac. & & \end{array} \tag{1}$$

Note that (1) says that $(A,+,0)$ is an abelian group.

Zero divisors and integral domains. An **integral domain** is a ring A such that for all $a,b \in A$, if $ab=0$ then $a=0$ or $b=0$; and such that $0 \neq 1$.

A nonzero element a of a ring A is called **zero divisor** if $ab=0$ for some $b \in A$. Thus, an integral domain is the same as a ring without zero divisors, such that $0 \neq 1$.

Units and fields. An element a of a ring A is called **invertible** or a **unit** if there exists $b \in A$ such that $ab=1$. If A is a ring, we write $A^\times$ for the set of units in A. Then $(A^\times,\cdot,1)$ is an abelian group. A **field** is a ring in which all nonzero elements are invertible, and $0 \neq 1$. Equivalently, it is a ring A such that $A^\times = A \smallsetminus \{0\}$.

Irreducible. An element a in a ring A is called **irreducible** if it is not a unit, and for all $b,c \in A$ such that $a=bc$ one has that b or c is a unit.

Ring homomorphisms. Let A,B be rings. A map $f\colon A \to B$ is a **ring homomorphism** if $f(a+b)=f(a)+f(b)$, $f(ab)=f(a)\,f(b)$ for all $a,b \in A$ and $f(1_A)=1_B$.

Polynomials. Let A be a ring and choose a symbol, say, X. We shall define a new ring $A[X]$. The elements of $A[X]$ are called **polynomials** over A in one variable X and $A[X]$ is called the polynomial ring.

An element of $A[X]$ is a sequence $(a_0,a_1,\ldots)$ of elements of A with only finitely many nonzero entries. An alternative and more usual notation is

$$(a_0,a_1,\ldots) = a_0 + a_1X + a_2X^2 + \cdots = \sum_{k\geq 0} a_kX^k.$$

We define addition and multiplication on $A[X]$ by

$$\begin{aligned} (a_0,a_1,\ldots)+(b_0,b_1,\ldots) &= (a_0+b_0,a_1+b_1,\ldots), \\ (a_0,a_1,\ldots)(b_0,b_1,\ldots) &= (c_0,c_1,\ldots) \end{aligned}$$

where $c_n = \sum_{k=0}^{n} a_k\, b_{n-k}$. In the usual notation:

$$\sum a_k X^k + \sum b_k X^k = \sum (a_k + b_k)\, X^k, \qquad \Big(\sum a_k X^k\Big)\Big(\sum b_k X^k\Big) = \sum c_k\, X^k$$

with c_n as before.

Let $f = \sum_k a_k X^k \in A[X]$. The elements $a_i \in A$ are called the **coefficients** of f. The **degree** $\deg f$ of f is the greatest $n \geq 0$ such that $a_n \neq 0$. The degree of the zero polynomial is defined to be $-\infty$. Note that nonzero constant polynomials have degree 0. If f is of degree n then a_n is called the **leading coefficient** and $a_n X^n$ the **leading term** of f. We call f **monic** if its leading term is 1.

There is an injective ring homomorphism $f\colon A \to A[X]$ defined by $f(a) = (a, 0, 0, 0, \ldots)$ in the unusual notation. We usually identify $f(a)$ with $a \in A$. The elements of $f(A)$ are called the constant polynomials in $A[X]$.

Examples. Every field is an integral domain, and every integral domain is a ring:

$$\{\text{fields}\} \subset \{\text{integral domains}\} \subset \{\text{rings}\}.$$

Theorem 2 (division with remainder for polynomials)**.** *Let $f, g \in K[X]$ be polynomials over a field K with $g \neq 0$. Then there are unique $q, r \in K[X]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.*

Proof. Existence. There exist $q, r \in K[X]$ such that $f = gq + r$ because one can put $q = 0$, $r = f$. Choose now q, r such that r has minimal degree and write $\deg(g) = \ell$, $\deg(r) = m$. We claim that $m < \ell$. Suppose that on the contrary $m \geq \ell$ and write $g = \sum_k a_k X^k$, $r = \sum_k b_k X^k$. Put

$$r_1 = r - g\, b_m\, a_\ell^{-1}\, X^{m-\ell}, \qquad q_1 = q + b_m\, a_\ell^{-1}\, X^{m-\ell}.$$

Then $f = g_1 q + r_1$ but $\deg(r_1) < \deg(r)$, contradicting the minimality of $\deg(r)$. This proves that $\deg(r) < \deg(g)$ and finishes the proof of the existence.

Uniqueness. Let (q_i, r_i) (for $i \in \{1, 2\}$) both satisfy the conditions of the proposition. Then $g \mid gq_1 - gq_2 = (f - r_1) - (f - r_2) = r_2 - r_1$ and $\deg(r_2 - r_1) < \deg(g)$. This implies $r_1 = r_2$ and thus proves uniqueness. □

1.2 Exercises

(1.1) Prove that every field is an integral domain.

(1.2) Give an example of a ring which is not an integral domain. Give an example of an integral domain which is not a field. Give an example of a field.

(1.3) Let A be a ring. Prove that $A[X]$ is a ring. What are 0 and 1 in $A[X]$?

(1.4) Explicitly divide $X^5 - X^3$ by $X^2 + 2$ with remainder. Also divide X^5 by $X^3 + 2X + 1$.

(1.5) Let $f\colon A \to B$ be a ring homomorphism.

(a) Prove that $f(0_A) = 0_B$.

(b) Prove that f is injective if and only if $f^{-1}(0_B) = \{0_A\}$.

(c) Prove that if A is a field and B is nonzero, then f is injective.

(1.6) Prove that every finite integral domain is a field.

1.3 Solving by radicals

Let K be a field and $f \in K[X]$. If $\alpha \in K$ is such that $f(\alpha) = 0$ then we call α a **zero** or a **root** of f.

Definition 3. A field K is **algebraically closed** if every nonconstant polynomial $f \in K[X]$ has a root in K.

So $\mathbb{R}$ is not algebraically closed (choose $f = x^2 + 1$).

Theorem 4. *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

Proof. This cannot be proved here. Clearly the proof needs some analysis, because the *definition* of $\mathbb{R}$ and $\mathbb{C}$ is analytic. The most common proof is done in complex analysis and uses the Cauchy residue theorem.

A later exercise outlines an almost entirely algebraic proof. The only analytic part of it is the knowledge that every polynomial $f \in \mathbb{R}[X]$ of odd degree has a real zero. □

Lemma 5. *Let K be an algebraically closed field. Let $f \in K[X]$ be monic of degree n. Then there exist $\alpha_1, \ldots, \alpha_n \in K$ such that*

$$f = \prod_{i=1}^{n} (X - \alpha_i). \tag{6}$$

Moreover, $\alpha_1, \ldots, \alpha_n$ are unique up to reordering.[(1)]

Proof. Existence. Induction on n. It's true for $n = 0$. Let $n > 0$. As K is algebraically closed, there exists $\alpha_n \in K$ such that $f(\alpha_n) = 0$. By division with remainder (theorem 2) we can write

$$f = (X - \alpha_n) \cdot g + r \tag{7}$$

with $g, r \in K[X]$ and $\deg r < \deg(X - \alpha_n) = 1$. So r is constant. Plugging α_n in for X in (7) gives $0 = f(\alpha_n) = r(\alpha) = r$. So $r = 0$ and $f = (X - \alpha_n) \cdot g$. By the induction hypothesis, we can write $g = \prod_{i=1}^{n-1}(X - \alpha_i)$ and we find (6).

Uniqueness. Induction on n. It's true for $n = 0$. Let $n > 0$ and assume

$$\prod_{i=1}^{n} (X - \alpha_i) = \prod_{i=1}^{n} (X - \beta_i). \tag{8}$$

[(1)] That is, if also $f = \prod_{i=1}^{n}(X - \beta_i)$ with $\beta_i \in K$ then there exists $\pi \in S_n$ such that $\beta_i = \alpha_{\pi(i)}$ for all i.

Choose here $X = \alpha_n$ to obtain $\prod_{i=1}^{n}(\alpha_n - \beta_i)$. So there exists i such that $\alpha_n = \beta_i$. After reordering the β_j we may assume that $\alpha_n = \beta_n$. Dividing (18) by $X - \alpha_n$ yields $\prod_{i=1}^{n-1}(X - \alpha_i) = \prod_{i=1}^{n-1}(X - \beta_i)$. By the induction hypothesis, $\beta_1, \ldots, \beta_{n-1}$ is a reordering of $\alpha_1, \ldots, \alpha_{n-1}$. Therefore, $\beta_1, \ldots, \beta_n$ is a reordering of $\alpha_1, \ldots, \alpha_n$. □

Note that in lemma 5 the α_i are not required to be distinct.

If $\alpha, \beta \in K$, $n > 0$ are such that $\alpha^n = \beta$ then we say that α is a **root** or **radical** of β.

Definition 9. Let K be a field. A subfield $L \subset K$ is called **radically closed** in K if for all $\alpha \in K$, $n > 0$, if $\alpha^n \in L$ then $\alpha \in L$.

In words, all radicals in K of elements of L are again in L.

If K is a field and $A \subset K$ any subset then there clearly exists a smallest radically closed subfield L of K containing A. Indeed, it is the intersection of all radically closed subfields of K containing A. We say that L is the **radical closure** in K of A.

Example 10. You know that the roots of a quadric $aX^2 + bX + c$ are[2]

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{11}$$

The expression (11) is obtained from a, b, c and field operations $(+, -, \times, \div)$ and radicals. More precisely, the expression (11) is in the radical closure of $\{a, b, c\}$.

Definition 12. Let K be an algebraically closed field and let $f \in K[X]$. We say that f is **solvable** or **solvable by radicals** if the radical closure of the set of coefficients of f contains all roots in K of f.

So example 10 shows that every quadric is solvable. In this chapter, we prove that all cubics and quartics are solvable. Later on we prove that some (most) quintics are not.

1.4 Symmetric polynomials

Let A be a ring and consider $A[T_1, \ldots, T_n]$, the ring of polynomials over A in n variables.

Definition 13. The kth **elementary symmetric function** $\sigma_k \in A[T_1, \ldots, T_k]$ is defined by

$$\sigma_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \prod_{j=1}^{k} T_{i_j}. \qquad \square$$

[2] Polynomials of degree (respectively) $2, 3, 4, 5$ are called (respectively) quadric, cubic, quartic, quintic.

Examples:

$$\sigma_0 = 1 = \text{a single choice of the empty product,}$$

$$\sigma_1 = T_1 + \cdots + T_n, \qquad \sigma_2 = \sum_{1 \le i < j \le n} T_i T_j, \qquad \sigma_n = T_1 \cdots T_n.$$

It is clear that

$$\prod_{i=1}^{n} (X + T_i) = \sum_{k=0}^{n} \sigma_k X^{n-k}.$$

The monic polynomial with roots $T_1, \ldots, T_n$ is therefore

$$\prod_{i=1}^{n} (X - T_i) = \sum_{k=0}^{n} (-1)^k \sigma_k X^{n-k}.$$

Definition 14. A polynomial $f \in A[T_1, \ldots, T_n]$ is called **symmetric** if $f = f\big(u(T_1), \ldots, u(T_n)\big)$ for all permutations u of $\{T_1, \ldots, T_n\}$.

It is clear that, as the name already suggests, the elementary symmetric polynomials σ_k are symmetric.

Remark 15. Let us say a bit more about definition 14.

Let $U = \mathrm{Sym}(\{T_1, \ldots, T_n\})$ be the symmetric group on $\{T_1, \ldots, T_n\}$, also known as the group of permutations of $\{T_1, \ldots, T_n\}$ (see **). For $f \in A[T_1, \ldots, T_n]$ and $u \in U$ we write $f \circ u := f\big(u(T_1), \ldots, u(T_n)\big)$. The map $f \mapsto f \circ u$ is then a ring automorphism of $A[T_1, \ldots, T_n]$ which extends the permutation u of the variables T_i.

The map

$$\begin{aligned} A[T_1, \ldots, T_n] \times U &\longrightarrow A[T_1, \ldots, T_n], \\ (f, u) &\longmapsto f \circ u = f\big(u(T_1), \ldots, u(T_n)\big) \end{aligned}$$

is an example of a **group action.** We say that the group U acts on $A[T_1, \ldots, T_n]$ by ring automorphisms. In a nutshell, this means that $f \circ (uv) = (f \circ u) \circ v$ and $(f \triangledown g) \circ u = (f \circ u) \triangledown (g \circ u)$ for all $f, g \in A[T_1, \ldots, T_n]$, $u, v \in U$, $\triangledown \in \{+, \times\}$.

Another way of saying that f is symmetric is that it is invariant under the U-action.

Theorem 16 (Main theorem on symmetric polynomials)**.** *Consider a symmetric polynomial $P \in A[T_1, \ldots, T_n]$. Then there exists a polynomial $f \in A[U_1, \ldots, U_n]$ such that*

$$P = f\big(\sigma_1(T_1, \ldots, T_n), \sigma_2(T_1, \ldots, T_n), \ldots, \sigma_n(T_1, \ldots, T_n)\big).$$

In words, P is a polynomial in the elementary polynomials in the T_i.

Example 17. Before proving theorem 16, we look at an example. The polynomial $\sum_i T_i^3$ is clearly symmetric. By theorem 16, it can be expressed in terms of the $\sigma_k = \sigma_k(T_1, \ldots, T_n)$. Let's do that explicitly. We have

$$\sigma_1^3 = \Big(\sum_i T_i\Big)^3 = \Big(\sum_i T_i^3\Big) + 3\Big(\sum_{i \ne j} T_i^2 T_j\Big) + 6\,\sigma_3,$$

$$\sigma_1\,\sigma_2 = \Big(\sum_i T_i\Big)\Big(\sum_{j<k} T_j\,T_k\Big) = \Big(\sum_{i\neq j} T_i^2\,T_j\Big) + 3\,\sigma_3$$

so

$$\sigma_1^3 - 3\,\sigma_1\,\sigma_2 = \Big(\sum_i T_i^3\Big) - 3\,\sigma_3 \quad \text{and} \quad \sum_i T_i^3 = \sigma_1^3 - 3\,\sigma_1\,\sigma_2 + 3\,\sigma_3.$$

Proof of theorem 16. We need some terminology. A **monomial** of degree k is an expression $T_1^{k_1}\cdots T_n^{k_n}$ such that $k = \sum_i k_i$. An A-linear combination of degree k monomials is called a homogeneous polynomial of degree k.

It is enough to prove the theorem if P is homogeneous, so suppose it is.

We define a total ordering $<$ on the set of degree k monomials as follows. It is called the lexicographic ordering. We put $T_1 < \cdots < T_n$. Write

$$u = u_1\cdots u_k, \qquad v = v_1\cdots v_k$$

where $u_i, v_i \in \{T_1,\ldots,T_n\}$ and $u_i \leq u_{i+1}$, $v_i \leq v_{i+1}$ for all i. Then $u < v$ if there exists j such that $(u_1,\ldots,u_{j-1}) = (v_1,\ldots,v_{j-1})$ but $u_j < v_j$.

We may write $P = \sum_u a_u\,u$ (a sum over degree k monomials u with $a_u \in A$). The **leading monomial** of P is the least u such that $a_u \neq 0$. Suppose the theorem is false. Among the counterexamples, let P be one with maximal leading monomial. This is a high-brow way of doing induction and works because there are only finitely many degree k monomials.

Let $u = T_1^{k_1}\cdots T_n^{k_n}$ be the leading monomial in P. We have $k_i \geq k_{i+1}$ for all i (interchanging T_i and T_{i+1} in the term $a_u u$ yields some term $a_v v$ with $a_v = a_u$ and $v \geq u$; this implies $k_i \geq k_{i+1}$).

We aim to compare the leading monomial of P with that of $Q := \sigma_1^{\ell_1}\cdots\sigma_n^{\ell_n}$. The leading monomial of Q is the product of the leading monomials of the factors which is

$$T_1^{\ell_1}(T_1T_2)^{\ell_2}\cdots(T_1\cdots T_n)^{\ell_n} = T_1^{\ell_1+\cdots+\ell_n}\,T_2^{\ell_2+\cdots+\ell_n}\cdots T_n^{\ell_n}$$

and which becomes equal to $u = T_1^{k_1}\cdots T_n^{k_n}$ by putting

$$\ell_n := k_n, \qquad \ell_i := k_i - k_{i+1} \quad (i < n).$$

Now P, Q have equal leading monomials. So $P - a_u Q$ has greater leading monomial than P. Therefore, $P - a_u Q$ is a polynomial in the σ_k. Also, Q is and therefore, P is. This contradiction finishes the proof. □

Definition 18. A tuple $(g_1,\ldots,g_k)$ with $g_i \in A[T_1,\ldots,T_n]$ for all i is called a **symmetric tuple** of polynomials if for every $u \in \mathrm{Sym}(t_1,\ldots,t_n)$ there exists $v \in S_k$ such that $g_i \circ u = g_{v(i)}$ for all i.

In words, the effect on the g_i of permuting the variables T_j is no more than a permutation of the g_i.

If g_i is symmetric for every i, then $(g_1,\ldots,g_k)$ is a symmetric tuple of polynomials; the converse is of course false.

The following is an obvious and very useful lemma.

Lemma 19 (plugging in a symmetric tuple)**.** *Let $(g_1,\ldots,g_k)$ be a symmetric tuple of polynomials, where $g_i \in A[T_1,\ldots,T_n]$ for all i. If $f \in A[U_1,\ldots,U_k]$ is symmetric then so is the element $f(g_1,\ldots,g_k)$ of $A[T_1,\ldots,T_n]$.* □

1.5 Quartic equations

Easier than proving that cubic equations are solvable is deducing from it that quartic equations are solvable. So we begin with the latter. In the rest of this chapter we work in $\mathbb{C}$.

Theorem 20. *Assume that cubic equations over $\mathbb{C}$ are solvable. Then so are quartic ones.*

Proof. Let $f = \sum_k a_k X^k$ be a monic polynomial of degree 4 over an algebraically closed field K. Let $L \subset K$ be the radical closure of the coefficients a_0, a_1, a_2, a_3. We need to prove that all roots of f are in L.

Call those roots $\alpha, \beta, \gamma, \delta$ (see lemma 5). So $f = (X-\alpha)(X-\beta)(X-\gamma)(X-\delta)$. We now view $\alpha\,\beta, \gamma, \delta$ as variables. Define polynomials $k_1, k_2, k_3 \in L[\alpha, \beta, \gamma, \delta]$ by

$$k_1 = (\alpha+\beta-\gamma-\delta)^2, \quad k_2 = (\alpha-\beta+\gamma-\delta)^2, \quad k_3 = (\alpha-\beta-\gamma+\delta)^2.$$

One immediately sees that (k_1, k_2, k_3) is a symmetric tuple of polynomials. For example, the permutation (α, β) takes k_2 to $(-\alpha+\beta+\gamma-\delta)^2 = k_3$, thanks to the second power! Lemma 19 tells us now that whenever $h \in L[u_1, u_2, u_3]$ is a symmetric polynomial, $h(k_1, k_2, k_3)$ is symmetric in $\alpha, \beta, \gamma, \delta$.

Consider the **auxiliary polynomial** $g = (X-k_1)(X-k_2)(X-k_3)$. Every coefficient of g is, up to a sign, an (elementary) symmetric polynomial in the k_i. Therefore, every coefficient of g is symmetric in $\alpha, \beta, \gamma, \delta$.

By the main theorem of symmetric polynomials (theorem 16) every coefficient of g is a polynomial in $\{\sigma_k(\alpha, \beta, \gamma, \delta)\}_k$, that is, in $\{a_k\}_k$ (because the coefficients a_k of f are, up to signs, the elementary symmetric polynomials in $\alpha, \beta, \gamma, \delta$). So $g \in L[X]$.

By the assumption that cubics are solvable, the roots k_i of g are in L. Define ℓ_1, ℓ_2, ℓ_3, m by

$$\begin{cases} \alpha+\beta-\gamma-\delta = \ell_1 \\ \alpha-\beta+\gamma-\delta = \ell_2 \\ \alpha-\beta-\gamma+\delta = \ell_3 \\ \alpha+\beta+\gamma+\delta = m. \end{cases} \tag{21}$$

Then ℓ_i is a square root of k_i and is therefore in L. Also, $m \in L$ because it is a symmetric polynomial in $\alpha, \beta, \gamma, \delta$.

The system (21) is a non-degenerate system of linear equations over L in unknowns $\alpha, \beta, \gamma, \delta$ and solving it shows that $\alpha, \beta, \gamma, \delta \in L$ as required. □

1.6 Roots of unity

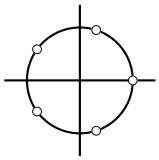
For $n \geq 1$ we have

$$\left\{ x \in \mathbb{C} \;\middle|\; x^n = 1 \right\} = \left\{ \exp\left(\frac{2\pi i k}{n}\right) \;\middle|\; 0 \leq k < n \right\}.$$

This set is written μ_n and its elements are called the nth (complex) roots of unity. See figure 1.

Note that $\mu_n \in \mathbb{C}^\times$ is a subgroup. It is a cyclic group of order n. Equivalently, it is isomorphic to the additive group of $\mathbb{Z}/n\mathbb{Z}$.

Figure 1. The five complex fifth roots of unity.



Definition 22. A **primitive n-th complex root of unity** is an $\alpha \in \mu_n$ which generates μ_n as a group.

The following are equivalent for a complex number α:

(a) α is a primitive n-th complex root of unity.

(b) $\alpha^n = 1$ but $\alpha^k \neq 1$ whenever $0 < k < n$.

(c) α is of the form $\exp\left(\frac{2\pi ik}{n}\right)$ with $k \in \mathbb{Z}$ coprime to n.

The number of primitive n-th complex roots of unity is written $\phi(n)$ and ϕ is known as the Euler totient function. In elementary number theory you learn that

$$\phi(n) = n \prod_{p|n} \frac{p-1}{p}$$

where the product is over the prime factors of n.

Definition 23. Let $n \geq 1$. The n-th **cyclotomic polynomial** ϕ_n is

$$\phi_n = \phi_n(X) := \prod_{\langle\alpha\rangle=\mu_n} (X - \alpha)$$

(product over the primitive n-th complex roots of unity). □

In exercise 12 you prove that $\phi_n \in \mathbb{Q}[X]$. It can be proved that ϕ_n is irreducible in $\mathbb{Q}[X]$ but we shall not use this result.

1.7 Cubic equations

Theorem 24. *Cubic polynomials over $\mathbb{C}$ are solvable. More precisely, every degree 3 polynomial over an algebraically closed field is solvable.*

Corollary 25. *Quartics over $\mathbb{C}$ are solvable.*

Proof of corollary 25 This is immediate from theorems 20 and 24. □

First proof of theorem 24 Our first proof is not entirely correct and mainly meant as something to marvel at. Consider a monic cubic $X^3 + aX^2 + bX + c$. On replacing X by $X - a/3$ one obtains a cubic of the form $f = X^3 + 3pX + 2q$ which it is therefore enough to solve. We claim that

$$\sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

is a root of f. Try it out and see that it works! Why aren't we entirely happy with this?

Second proof of theorem 24 The second proof is more correct and also shows how one might have discovered it.

As in the first proof, we only need to solve $f = X^3 + 3pX + 2q$. By lemma 5 there are (unique) $\alpha, \beta, \gamma \in K$ such that $f = (X-\alpha)(X-\beta)(X-\gamma)$. We need to prove that α, β, γ are in the radical closure $L \subset K$ of $\{p, q\}$. Let $\omega \in K$ be a primitive cube root of unity. Of course, $\omega \in L$.

We next treat α, β, γ as variables. Consider polynomials $u, v \in L[\alpha, \beta, \gamma]$ defined by

$$u = \alpha + \omega\beta + \omega^2\gamma, \quad v = \alpha + \omega^2\beta + \omega\gamma.$$

Claim: (u^3, v^3) is a symmetric tuple of polynomials (see definition 19). Proof of claim. It is (assumed to be) known that the symmetric group on α, β, γ is generated by $\{\pi_2, \pi_3\}$ where π_2 is the 2-cycle (β, γ) and π_3 is the 3-cycle (α, β, γ). Therefore, it is enough to show that u^3, v^3 are (at most) permuted under π_3 and π_2.

We have $u \circ \pi_2 = v$ and $v \circ \pi_2 = u$. That is, π_2 interchanges u with v. So it interchanges u^3 with v^3 as required.

We have

$$\begin{aligned} u \circ \pi_3 &= (\alpha + \omega\beta + \omega^2\gamma) \circ \pi_3 \\ &= \beta + \omega\gamma + \omega^2\alpha = \omega^2(\alpha + \omega\beta + \omega^2\gamma) = \omega^2 u \end{aligned}$$

and likewise $v \circ \pi_3 = \omega v$. In particular, π_3 preserves u^3 and v^3. The claim is proved.

Lemma 19 and the claim imply that whenever $h \in A[y_1, y_2]$ is a symmetric polynomial, $h(u^3, v^3)$ is symmetric in α, β, γ.

Consider the **auxiliary polynomial** $g = (X - u^3)(X - v^3) \in K[x]$. Any coefficient of g is, up to a sign, an elementary symmetric function in u^3, v^3 and therefore symmetric in α, β, γ. By the main theorem on symmetric functions (theorem 16) we find $g \in L[\sigma_2(\alpha, \beta, \gamma), \sigma_3(\alpha, \beta, \gamma)][X] = L[p, q][X] = L[X]$.

From now we treat α, β, γ as numbers. The polynomial g has degree 2 and is therefore solvable by example 10, that is, $u^3, v^3 \in L$. As L is closed under taking cube roots we have $u, v \in L$. We have a non-degenerate system of linear equations over L in unknowns α, β, γ

$$\begin{cases} \alpha + \quad \beta + \quad \gamma = 0 \\ \alpha + \omega\beta + \omega^2\gamma = u \\ \alpha + \omega^2\beta + \omega\gamma = v \end{cases}$$

and "solving" it for α, β, γ shows that $\alpha, \beta, \gamma \in L$ as well as required. □

1.8 How to use Maple

This is not part of the course, but I recommend doing it. At a unix terminal, type maple; you get a clever logo, and the prompt >. For example, you can

calculate $\sum T_i^3$ in terms of elementary symmetric functions by the following few lines:

```
> s1:=a+b+c; s2:=a*b+a*c+b*c; s3:=a*b*c;

                 s1 := a + b + c
                 s2 := a b + a c + b c
                 s3 := a b c

> expand(a^3+b^3+c^3-s1^3);

      2       2        2                2     2        2
  - 3 a b - 3 a c - 3 a b - 6 a b c - 3 a c - 3 b c - 3 b c

> expand(%+3*s1*s2);

                  3 a b c

> evalb(expand(s1^3-3*s1*s2+3*s3) = a^3+b^3+c^3);

                   true
```

Mathematica is very similar.

1.9 Exercises

(1.6) If $f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$ has roots $\alpha_1, \ldots, \alpha_n$, what polynomial has roots $c\alpha_1, \ldots, c\alpha_n$?

(1.7) Let $a, b, c \in \mathbb{C}$. Let K be the radical closure of $\{a, b, c\}$ (that is, the smallest subfield of $\mathbb{C}$ containing a, b, c and such that for all $\alpha \in \mathbb{C}$, $n > 0$, if $\alpha^n \in K$ then $\alpha \in K$). Let L be the radical closure of $\{ab, bc, ca\}$. Prove $K = L$.

(1.8) Prove that $X^5 - 3X^3 - 8$ is solvable by radicals.

(1.9) Let $T_1, \ldots, T_n$ be variables. Express the polynomial

$$S = \sum_{1 \le i < j < k \le n} T_i\, T_j\, T_k\, (T_i + T_j + T_k)$$

in terms of the elementary symmetric polynomials $\sigma_k(T_1, \ldots, T_n)$.

(1.10) Express each of the following in terms of the σ_k:

$$\sum_i T_i^2, \qquad \sum_{i,j} T_i^2\, T_j, \qquad \sum_{i<j} T_i^2\, T_j^2.$$

(1.11) Let α, β, γ be the roots of the equation $X^3 + pX^2 + q = 0$. Find the cubic polynomial equation whose roots are $\alpha^3,\ \beta^3,\ \gamma^3$.

(1.12) Recall the cyclotomic polynomial $\phi_n(X) := \prod(X - \alpha)$ where the product is over the complex primitive n-th roots of unity.

(a) Prove $\prod_{d|n} \phi_d(X) = X^n - 1$ for all $n \ge 1$. Here, the product is over the positive divisors d of n.

(b) Prove $\phi_n(X) \in \mathbb{Q}(X)$.

(c) Prove $\phi_n(X) \in \mathbb{Q}[X]$.

(1.13) Write $\varepsilon := \exp(2\pi i/5)$ for the natural primitive 5th root of 1; it is a root of the quartic $f(X) = X^4 + X^3 + X^2 + X + 1$. Find the quadratic equation whose two roots are $\varepsilon + \varepsilon^4$ and $\varepsilon^2 + \varepsilon^3$, and hence give radical formulas for $\cos(2\pi/5)$ and $\cos(4\pi/5)$.

(1.14) Let $S_k = \sum_i T_i^k$ be the power sum. Express S_k in terms of the elementary symmetric polynomials if $k = 4, 5$. Do it for $k = 6, 7$ if you know how to use Maple or Mathematica.

(1.15)

(a) Put $f = X^6 + a\,X^5 + a\,X + 1 \in \mathbb{C}[X]$. Find an explicit $g \in \mathbb{C}[y]$ such that $X^{-3}f(X) = g(X + X^{-1})$. Prove that f can be solved by radicals.

(b) Prove or disprove the following. Put $h = X^5 + a\,X^4 + a\,X + 1 \in \mathbb{C}[X]$. Then h can be solved by radicals.

(1.16) Let $L = \mathbb{C}(T_1, \ldots, T_n)$ be the field of rational functions in n variables. Let the symmetric group S_n act on L by permutation of the variables T_i. Let $\sigma_k \in L$ be the elementary symmetric polynomials in the T_i. Put

$$K = \{f \in L \mid r(f) = f \text{ for all } r \in S_n\},$$
$$M = \mathbb{C}(\sigma_1, \ldots, \sigma_k) \subset L.$$

In other words, M is the smallest subfield of L containing $\mathbb{C}$ and the T_i. Prove that $K = M$.

(1.17) Prove Newton's rule $\sum_{k=0}^{n}(-1)^k \sigma_k\, S_{n-k} = 0$ where $S_k = \sum_i T_i^k$ is the power sum.

(1.18) Let σ_i be the elementary symmetric functions of $T_1, \ldots, T_n$ and τ_i the elementary symmetric functions of $T_1^2, \ldots, T_n^2$. Prove:

$$\tau_k = \sum_{i=0}^{2k} (-1)^{k+i}\, \sigma_i\, \sigma_{2k-i}.$$