15. Cubics, Quartics and Polygons

It is interesting to chase through the arguments of §14 and see how this affects solving polynomial equations in specific examples. We make a global assumption that the characteristic is neither 2 nor 3.

Lemma 15.1. *Let $f(x) \in K[x]$ be a separable polynomial of degree n.*

Then the Galois group is a subgroup of S_n, the permutations of the roots.

Proof. Clear, since any automorphism of a splitting field is determined by its action on the roots. □

Now $A_n \subset S_n$ and so $H = G \cap A_n \subset G$ is either equal to G or of index two. If we have the latter, by the Fundamental Theorem, it follows that there is a quadratic extension M/K. Since this is universally true, no matter which field we start with, we might well expect that there is some universal formula which determines M.

Definition 15.2. *Let $f(x) \in K[x]$ be a polynomial, in which $f(x)$ splits as*

$$f(x) = \lambda(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha).$$

*The **discriminant** Δ is the square of the product*

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j).$$

Lemma 15.3. *Let $f(x) \in K[x]$ be a polynomial with splitting field L/K and discriminant $\Delta \in L$.*

Then $\Delta \in K$ and $\Delta = 0$ if and only if $f(x)$ has a repeated root. Moreover if $\Delta \neq 0$ then $x^2 - \Delta$ splits in $K[x]$ if and only if the Galois group is a subgroup of A_n.

Proof. The second statement is immediate. If $\Delta \neq 0$, then $f(x)$ is surely separable and so L/K is Galois.

We already know that δ is invariant under the action of A_n and that an arbitrary element of S_n fixes δ up to sign. Thus $\Delta = \delta^2$ lies in the fixed field of G, which by the Fundamental Theorem of Galois Theory is equal to K.

Finally $x^2 - \Delta$ splits in K if and only if $\delta \in K$ if and only if δ is invariant under G if and only if $G \subset A_n$. □

We turn to the calculation of the discriminant.

Definition 15.4. *Let K be a field and let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be n scalars. The determinant*

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \ldots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \ldots & \lambda_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_n^{n-1} \end{vmatrix}$$

is known as the ***Vandermonde determinant****.*

Lemma 15.5. *The Vandermonde determinant is equal to*

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \ldots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \ldots & \lambda_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_n^{n-1} \end{vmatrix} = \prod_{i<j} (\lambda_i - \lambda_j).$$

Proof. First note that we may replace λ_i by the variable x_i. In this case both sides are polynomials in $x_1, x_2, \ldots, x_n$ and so both sides are elements of the ring $R = K[x_1, x_2, \ldots, x_n]$. By unique factorisation and considerations of degree it suffices to check that $x_i - x_j$ is a factor of the LHS and that the constant coefficients match up. The latter is an easy check.

To check that $x_i - x_j$ divides the LHS, it suffices to check that the LHS vanishes when $\lambda_i = \lambda_j$. But this is clear, as then we are taking the determinant of a matrix with two equal columns. □

Remark 15.6. *The Vandermonde determinant provides a slick way of checking that A_n is a normal subgroup. The key point to check is that a transposition, acting on δ, switches the sign. But this is clear, looking at the LHS, since the determinant changes sign, when one switches two columns.*

$$
\begin{aligned}
\Delta &= \delta^2 \\
&= \delta \cdot \delta \\
&= \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} \\
&= \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{vmatrix},
\end{aligned}
$$

where we used the fact that taking transposes does not affect the determinant.

The last product can be computed by first multiplying the matrices together and then computing the determinant, as

$$\det(AB) = \det A \det B.$$

Rather than write down the general formula, it is perhaps more interesting to compute in some relatively simple cases.

If $n = 2$ we get

$$\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 1 & \beta \end{pmatrix} = \begin{pmatrix} 2 & \alpha + \beta \\ \alpha + \beta & \alpha^2 + \beta^2 \end{pmatrix}.$$

Suppose

$$f(x) = x^2 + ax + b = (x - \alpha)(x - \beta).$$

Multiplying out we get

$$\begin{aligned}
(x - \alpha)(x - \beta) &= x^2 - (\alpha + \beta)x + \alpha\beta \\
&= x^2 + ax + b,
\end{aligned}$$

so that comparing coefficients, we have

$$\alpha + \beta = -a \qquad \text{and} \qquad \alpha\beta = b.$$

$$\begin{aligned} a^2 &= (\alpha+\beta)^2 \\ &= \alpha^2+\beta^2+2\alpha\beta \\ &= (\alpha^2+\beta^2)+2b. \end{aligned}$$

So

$$\alpha^2+\beta^2 = a^2-2b.$$

Thus Δ is equal to

$$\begin{vmatrix} 2 & -a \\ -a & a^2-2b \end{vmatrix} = 2(a^2-2b)-a^2 = a^2-4b,$$

which should look familiar.

One can make a similar computation for cubics. In this case we have

Proposition 15.7. *Let $f(x) \in K[x]$ be an irreducible cubic.*

Then the Galois group is isomorphic to A_3 if $x^2-\Delta$ splits in K and is equal to S_3 otherwise.

Proof. The Galois group is a transitive subgroup of S_3, of which there are only two, A_3 and S_3. But $G \subset A_3$ if and only if $x^2-\Delta$ splits in K. □

This gives us a method to solve the cubic. First compute the intermediate field M corresponding to A_3, that is, adjoin the square root of Δ. The resulting field extension L/M has Galois group isomorphic to $\mathbb{Z}_3$, thus there ought to be an expression involving δ and the coefficients of the cubic, for which we need to take a cube root.

We now apply a similar technique for quartics.

Proposition 15.8. *Let $f(x) \in K[x]$ be an irreducible quartic.*

Then the Galois group is isomorphic to one of

(1) S_4,
(2) D_4,
(3) $\mathbb{Z}_4$
(4) A_4, or
(5) $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

The latter two occur if and only if $x^2-\Delta$ splits in K.

Proof. These are only the only transitive subgroups of S_4. □

Once again, this ought to yield a method to solve the quartic. First adjoin δ, the square root of Δ, to reduce the Galois group to A_4. Now use the fact that $V \subset A_4$ is a normal subgroup, with quotient $\mathbb{Z}_3$, to find a further field extension, that is obtained by adjoining appropriate

cube roots. This reduces the Galois group to $\mathbb{Z}_2 \times \mathbb{Z}_2$. The remaining field extension is obtained by adjoining successive square roots.

Thus the general form of a solution to a quartic equation, involves taking square roots and cube roots only. In practice determining these formulas is somewhat involved and uninspiring. A much more interesting question is to determine those regular polygons which are constructible.

Lemma 15.9. *The regular n-gon is constructible if and only if the angle $\frac{2\pi}{n}$ is constructible.*

Proof. Suppose the regular n-gon is constructible. Then the angle subtended at the centre of the n-gon (which is surely constructible) by two adjacent vertices is $\frac{2\pi}{n}$.

Conversely suppose we can construct the angle $\frac{2\pi}{n}$. Then we can construct the angles

$$a\frac{2\pi}{n}.$$

Place points on the unit circle with the above angles and simply join up the points. □

Lemma 15.10. *If the regular polygon with nm sides is constructible then the regular polygons with n sides and m sides are constructible. Further if m and n are coprime, the converse holds.*

Proof. One direction is clear. If you can construct the regular polygon with nm sides, then you can certainly construct the regular polygon with n and m sides.

Now suppose that m and n are coprime. Then there are integers a and b such that

$$1 = am + bn,$$

so that

$$\frac{1}{mn} = \frac{a}{n} + \frac{b}{m}.$$

By assumption we can construct the angles

$$\frac{2\pi}{n} \qquad \text{and} \qquad \frac{2\pi}{m},$$

and so we can construct

$$\frac{2\pi}{mn} = a\frac{2\pi}{n} - b\frac{2\pi}{m}.$$

But then the mn-gon is contructible. □

Using (15.10), to answer the question of which n-gons are constructible, we only need to consider the case when n is a power of a prime. Since we can bisect any angle, we can certainly construct any 2^k-gon.

Now constructing the angle $2\pi/n$ is basically the same as showing that a primitive nth root of unity has degree a power of two over $\mathbb{Q}$.

Lemma 15.11. *The angle $\theta = 2\pi/n$ is contructible if and only if the degree of the mininum polynomial of $\omega = e^{2\pi i/n}$ is a power of two.*

Proof. The angle θ is constructible if and only if the lengths $\alpha = \cos\theta$ and $\sin\theta$ are constructible. So if the angle θ is constructible, then the degree of the minimum polynomial of α is a power of two. Now

$$\omega + \bar{\omega} = 2\alpha.$$

As $\bar{\omega} = \omega^{-1}$, we have

$$\omega^2 - 2\alpha\omega + 1 = 0.$$

So ω is a root of the polynomial

$$x^2 - 2\alpha x + 1 \in \mathbb{Q}(\alpha)[x].$$

Thus the degree of ω over $\mathbb{Q}(\alpha)$ is either one or two. Now apply the Tower Law. □

Note that ω is a primitive root of unity.

Lemma 15.12. *Let ω be a primitive p^k-th root of unity, where p is an odd prime.*

If ω has degree a power of two over $\mathbb{Q}$ then $k = 1$ and $p = 2^s + 1$, for some s.

Proof.

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1.$$

So the degree of ω, in the case $k = 1$, is

$$p - 1.$$

As this is a power of two, we have $p = 2^s + 1$.

Now if $k > 1$, we may as well assume that $k = 2$. Now

$$x^{p^2} - 1 = \Phi_1(x)\Phi_p(x)\Phi_{p^2}(x).$$

So

$$p^2 = 1 + (p-1) + d,$$

where d is the degree of ω. Thus $d = p^2 - p = p(p-1)$, which is never a power of two. □

Lemma 15.13. *Let p be a prime of the form*

$$2^s + 1.$$

Then s is a power of two.

Proof. Suppose not. Then we could write $s = ab$, where a is odd. Now

$$x^a + 1 = (x + 1)(x^{a-1} - x^{a-2} + \dots).$$

But then

$$p = (2^b)^a + 1,$$

would not be prime. □

Theorem 15.14. *The regular n-gon is constructible if and only if*

$$n = 2^k p_1, p_2, \dots, p_m,$$

where $p_1, p_2, \dots, p_m$ are distinct odd primes of the form $2^{2^k} + 1$.

Proof. By what we have already proved, it suffices to consider the case n is an odd prime, of the form $2^{2^k} + 1$, and we only need to prove that the corresponding angle is constructible.

Consider the Galois group G of $x^n - 1$. This is abelian, isomorphic to $U_{2^{2^k}}$. The order of this group is

$$2^{2^k} - 2^{2^k - 1} = 2^{2^k - 1},$$

a power of two. Thus G is a 2-group and we can filter a splitting field $\mathbb{Q}(\omega)/\mathbb{Q}$ by intermediary fields, all of which are quadratic extensions of the previous field. Thus we can do the same for the subfields,

$$\mathbb{Q}(\cos\theta) \qquad \text{and} \qquad \mathbb{Q}(\sin\theta).$$

But then $\cos\theta$ and $\sin\theta$ are constructible, which is what we want. □