Galois Theory

Arnau Mas

2019

These are notes gathered during the subject *Teoria de Galois* as taught by Francesc Perera between September 2019 and January 2020.

Chapter 1

Preliminaries

1.1 The solution of low degree polynomial equations

It is surely well-known to any aspiring mathematician that there exist no general formulas for the solutions of polynomial equations of degree five and higher. This implies, of course, that such formulas exist for equations of degree fourth and lower. Indeed, the solution of linear equations is trivial and the quadratic formula should be more than well-known by this point. In this section we present a derivation of the solutions of both the quadratic and cubic equations.

1.1.1 The quadratic equation

First, note that we can, without loss of generality, assume that we are working with a monic equation since we may always divide through by the leading coefficient to obtain an equation with the same solutions and with leading coefficient 1. Thus, we are trying to solve $x^2 + bx + c = 0$. The standard method is completing the square, that is to write $x^2 + bx + c$ as a square, and one achieves so by adding and substracting $\frac{b^2}{4}$:

$$x^2 + bx + c = x^2 + bx + \frac{b^2}{4} - \frac{b^2}{4} + c = \left(x + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c.$$

Then the solutions to the original equation must satisfy

$$\left(x + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c.$$

If the term on the right is not a square in the field we are working over then there are no solutions in that field. On the other hand, if it is a square then it has two

square roots and the solutions to the original equation are

$$x = -\frac{b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c},$$

which is the well known quadratic formula.

1.1.2 The cubic equation

Less well-known is the formula for the solutions of the cubic equation. Whereas the quadratic formula had been known to the greeks and babylonians, the cubic formula was discovered later during the fifteenth century. There were several italian mathematicians involved in its discovery: Cardano, Ferrari and del Ferro among others. The question of the original discoverer is a contemptious matter.

The first step in the solution is a change of variables to eliminate the quadratic term. If $x = y - \frac{1}{3}b$ then the original (monic) polynomial becomes

$$\begin{aligned} x^3 + bx^2 + cx + d &= y^3 - by^2 + \frac{1}{3}b^2y - \frac{1}{27}b^3 + by^2 - \frac{2}{3}b^2y + \frac{1}{9}b^3 + cy - \frac{1}{3}bc + d \\ &= y^3 + \left(c - \frac{1}{3}b^2\right)y + \frac{2}{27}b^3 - \frac{1}{3}bc + d. \end{aligned}$$

Therefore we only need to be able to solve cubics of the form $x^3 + px + q = 0$.

The basic trick is similar to completing the square. We have the identity

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + 3uv(u+v) + v^3,$$

and rearranging we obtain $(u+v)^3 - 3uv(u+v) - u^3 - v^3 = 0$. One then notices that there are cubic and linear terms in $u+v$ but no quadratic terms. Then one tries to solve for u and v to then obtain x as $u+v$. u and v must satisfy $-3uv = p$ and $-u^3 - v^3 = q$. Multiplying this second condition by u^3 we get

$$u^6 + qu^3 + u^3v^3 = 0,$$

and using the fact that $uv = -\frac{1}{3}p$ we arrive at

$$u^6 + qu^3 - \frac{p^3}{27} = 0,$$

which is quadratic in u^3. If we instead had multiplied through by v^3 we would have arrived to the same equation for v^3 instead.

Up to now nothing we have done relied on any additional assumption on the field have been working over. From this point, however, the nature of the solutions

will depend on the behaviour of radicals in the field in question. We will assume we are working in $\mathbb{C}$. We can then solve for u^3 and v^3 to find

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
$$v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

The ambiguity with the signs is eliminated due to the fact that $u^3 + v^3 = -q$ so we find the only good options are those in which the signs of the square root terms are opposite, so that they will cancel when added. Since we only care about the sum of u and v we might as well choose

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

There are three possibilities for u and three for v. Indeed, every complex number has three roots and if a is one of them then so are ωa and $\omega^2 a$ where $\omega = e^{\frac{2\pi}{3}i}$. Not every combination of them leads to a solution of the cubic —if it were so we would have more than three roots and a cubic polynomial can only have three roots— since they are constrained by the relation $3uv = -p$. So, once we find u and v that satisfy this then so will ωu and $\omega^2 v$, as well as $\omega^2 u$ and ωv since $\omega^3 = 1$.

All together, one of the solutions to the cubic $x^3 + px + q = 0$ is given by

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

which is known as Cardano's formula. If we undo the change of variable to eliminate the quadratic term and use $p = c - \frac{1}{3}b^2$ and $q = \frac{2}{27}b^3 - \frac{1}{3}bc + d$ then we obtain the cubic formula in all of its glory:

$$x = -\frac{b}{3} + \sqrt[3]{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right) + \sqrt{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right)^2 + \left(\frac{c}{3} - \frac{b^2}{9}\right)^3}}$$
$$+ \sqrt[3]{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right) - \sqrt{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right)^2 + \left(\frac{c}{3} - \frac{b^2}{9}\right)^3}}.$$

1.2 Polynomial rings

The study of polynomial rings is particularly important in Galois theory since they play an important role in many of the constructions and definitions of the theory. Of special relevance is the study of their quotient rings.

1.2.1 The universal property of polynomial rings

Given a ring[1] R its polynomial ring $R[x]$ can be defined in various ways. Most commonly, the elements of $R[x]$ are said to be "formal sums" of the form

$$\sum_{k=1}^{n} a_k x^k$$

where the a_k are elements of R and x is refered to as an "indeterminate" or some other similarly ambiguous term. This definition may feel imprecise to the more technically inclined reader. A more exact definition of $R[x]$ is as the set of sequences of elements of R with finite suport. The sum is defined pointwise and the product is defined in a convoluted manner which correspond to the way one would multiply polynomials with repeated application of the distribuitive law. Then there is a canonical inclusion $R \hookrightarrow R[x]$ by way of $a \mapsto (a, 0, \cdots)$. And if we define x to be the sequence $(0, 1, \cdots)$ then we recover the more standard presentation of $R[x]$.

This discussion, however, is about what a programmer would call the implementation details and it misses the bigger picture. How $R[x]$ is constructed is not really what is relevant here. It is much more illuminating to think about what we want out of $R[x]$ instead. For one, $R[x]$ should contain R. We could require $R \subseteq R[x]$, but let's be more general and allow for an injective morphism $\iota\colon R \hookrightarrow R[x]$ that picks out a copy of R inside $R[x]$. The other important aspect of $R[x]$ is the indeterminate. The way to formalize it is with what is known as a universal property: for any morphism $\phi\colon R \to S$ and distinguished element $s \in S$ there is a unique morphism $\tilde{\phi}\colon R[x] \to S$ such that $\tilde{\phi} \circ \iota = \phi$ and $\tilde{\phi}(x) = s$. That is, $\tilde{\phi}$ must agree with ϕ on R and it must send x to s. This does indeed uniquely determine $\tilde{\phi}$. It can be shown that this determines $R[x]$ up to unique isomorphism, meaning there is a unique isomorphism between any two rings that satisfy the universal property. So you can construct $R[x]$ in whatever way you like so long as the result satisfies the universal property.

[1] We will always assume that we are dealing with commutative rings with identity unless otherwise stated.

One last remark about polynomial rings in many variables: once we have defined the polynomial ring of a ring $\mathbb{R}$, we can then proceed inductively to define the polynomial ring on n variables as $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$. Polynomial rings in more than one variables also satisfy a universal property, which is essentially the same as before except now we have to specify where $\tilde{\phi}$ sends all of the x_i.

This universal property is not just of theoretical importance, it is also extermely practical. Indeed, it provides a very quick way of specifying morphisms on a polynomial ring. All you need is to specify how it acts on the coeficients and where it sends the indeterminate and you're done.

Example 1.1. These are various examples of morphisms defined on a polynomial ring making use of the universal property.

(*i*) For any element $\alpha \in R$ we can define the evaluation morphism $\mathrm{ev}_\alpha \colon R[x] \to R$ such that $\mathrm{ev}_\alpha|_R = \mathrm{id}_R$ and $\mathrm{ev}_\alpha(x) = \alpha$. That is, simply evaluate a polynomial on the element $\alpha \in R$. The element we evaluate at need not be an element of R, in fact it can be an element of any ring which contains R.

(*ii*) A trick that is often used when working with polynomials is a change of variable. This idea can be made formal in terms of an automorphism of $R[x]$. Say we wanted to make the change $y = x + 1$, or $x = y - 1$. This amounts to defining a morphism $\phi \colon R[x] \to R[x]$ such that $\phi|_R = \mathrm{id}_R$ and $\phi(x) = y - 1$. ϕ does not move the coeficients and changes x to $y - 1$. More generally, we could perform a change of the form $\phi(x) = ay + b$. In order for ϕ to be an isomorphism, a must be invertible. Indeed, ϕ^{-1} sends x to $a^{-1}(x - b)$. Then, when showing that a certain polynomial is irreducible, for instance, we can do any change of variable we please and rest assured that the resulting polynomial will be irreducible if and only if the original one was irreducible, for irreducibility is preserved under isomorphism.

(*iii*) Any permutation $\sigma \in \mathfrak{S}_n$ induces an isomorphism on $R[x, \ldots, x_n]$ by permuting the variables according to σ. Indeed, let ϕ_σ be the unique morphism that is the identity on R and such that $\phi_\sigma(x_i) = x_{\sigma(i)}$. You can check that $\phi_\sigma \circ \phi_\tau = \phi_{\sigma\circ\tau}$. And as a corollary $\phi_\sigma^{-1} = \phi_{\sigma^{-1}}$. This is in fact an action of the symmetric group $\mathfrak{S}_n$ on $R[x_1, \cdots, x_n]$. The polynomials invariant under this action, $R[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ are known as the *symmetric polynomials*.

$\triangledown$

Chapter 2

Field extensions

2.1 Definition and examples

Definition 2.1 (Field extension)**.** We say a field F is an *extension* of a field K if K is a subfield of F. More generally, given any field K and an injective morphism $\iota\colon K \hookrightarrow F$ we will refer to the situation as a field extension and often identify K with $\iota(K)$ and simply write $K \subseteq F$. △

There are some immediate examples of field extensions such as $\mathbb{R} \subseteq \mathbb{C}$ and $\mathbb{Q} \subseteq \mathbb{R}$. In the following examples we detail the construction of three related kinds of extensions.

2.1.1 Simple extensions

Say we already have an extension $K \subseteq F$ and an element $\alpha \in F$. Then we can define the evaluation on α morphism, ev_α. Since $K[x]$ is a PID there must exist a polynomial $p(x) \in K[x]$ such that $\ker(\mathrm{ev}_\alpha) = \langle p(x) \rangle$. If we denote $\mathrm{im}(\mathrm{ev}_\alpha)$ by $K[\alpha]$ we have, by the Isomorphism Theorem

$$K[\alpha] \cong K[x]/\langle p(x) \rangle.$$

We also have $K \subseteq K[\alpha]$. Indeed, the image of a constant by ev_α is itself, so $K \subseteq \mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha]$. We can then consider the set $K(\alpha)$ which is the union of $K[\alpha]$ and the inverses of all of its nonzero elements —they exist since $K[\alpha] \subseteq F$—. This is isomorphic to the field of fractions of $K[\alpha]$. Thus we have $K \subseteq K[\alpha] \subseteq K(\alpha)$, meaning $K(\alpha)$ is a field extension of K. From the

Various things can happen with $K(\alpha)$. For one, if $\alpha \in K$ then $\mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha] = K$, which is to be expected since α was already in α. In this case then

$\ker(\mathrm{ev}_\alpha) = \langle x - \alpha) \rangle$, which is essentially the fact that a polynomial has α as a root if and only if it is divisible by $(x - \alpha)$.

If ev_α has a nontrivial kernel then it follows that its generator is irreducible. Indeed, since $K[x]/\langle p(x) \rangle \cong K[\alpha]$ and $K[\alpha]$ is a domain then $p(x)$ is prime, and therefore irreducible. This means that $\langle p(x) \rangle$ is a maximal ideal and $K[\alpha]$ is a field, so in this case $K[\alpha] = K(\alpha)$. If this is the case we say the element α is *algebraic* over K. The generator of $\ker(\mathrm{ev}_\alpha)$ is not unique, since any scalar multiple of a generator is also a generator. However, there is always a unique *monic* generator, which is called the *minimal polynomial of* α *over* K, written $m_{\alpha,K}(x)$ or simply $m_\alpha(x)$ if the base field is understood.

If, instead, ev_α has a trivial kernel then $K[\alpha] \cong K[x]/\{0\} \cong K[x]$ and so $K(\alpha) \cong K(x)$. This means that adding α to K is essentially like adding a free variable. We say α is *transcendental* over K. We will analyse the difference between this two cases later on.

Extensions of this sort are called *simple extensions* and α is called a *primitive element* of the extension.

2.1.2 Quotient of a polynomial ring by a maximal ideal

This is a way of constructing what are essentially simple extensions without requiring the prior existence of a primitive element in a larger extension.

The polynomial ring $K[x]$ is a PID which means that the ideal generated by an irreducible polynomial $p(x)$, $\langle p(x) \rangle$ is a maximal ideal. This in turn means that the quotient $F = K[x]/\langle p(x) \rangle$ is a field. Not only that, F is in fact a field extension of K. Let's see how we can construct an inclusion $F \hookrightarrow K$.

We have at our disposal an inclusion $\iota \colon K \hookrightarrow K[x]$ and a projection $\pi \colon K[x] \twoheadrightarrow F$. Since any two elements of K belong to different equivalence classes the restriction of π to K is injective, which means the composition $\pi \circ \iota \colon K \to F$ is also injective. Thus F is an extension of K.

We may summarise this in the following lemma.

Lemma 2.1. *Let K be a field and $p(x) \in K[x]$ an irreducible polynomial. Then the quotient $K[x]/\langle p(x) \rangle$ is a field extension of K.*

A number of extensions are of this form. Indeed, we have that $\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$ and the class of x is written i. There is also the extension $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$, which is typically written $\mathbb{Q}(\sqrt{2})$. More generally, if b is not a square in $\mathbb{Q}$ then $x^2 - b$ is irreducible and we have the extension $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}[x]/\langle x^2 - b \rangle$.

By this process we have enlarged the field K by "artificially" adding a primitive element. Indeed, if $p(x) = \sum_{k=0}^{n} a_k x^k$ in the quotient we have

$$0 = \overline{p(x)} = \overline{\sum_{k=0}^{n} a_k x^k} = \sum_{k=0}^{n} a_k \overline{x}^k \tag{2.1.1}$$

so $\bar{x}$, the class of x, is a root of $p(x)$. Note that in eq. (2.1.1) we abused notation and wrote what should have been $\overline{a_k}$ simply as a_k. As we mentioned, the equivalence class of a constant does not contain any other constant so we can, and will, get away with this abuse of notation.

Conversely, a simple extension $K(\alpha)$ is isomorphic to $K[x]/\langle m_\alpha \rangle$ if α is algebraic, essentially by definition.

2.1.3 Subfield generated by a set

Given an existing extension $K \subseteq F$ and a set $S \subseteq F$ we define $K[S]$ to be the smallest subring of F containing K and X, and then $K(S)$ as the result of adding to $K[S]$ the inverses of all its nonzero elements. This is, by construction, the smallest subfield of F that contains both K and S. Notice that $K(\{\alpha\})$ coincides with the simple extension $K(\alpha)$ we described in the previous section. Indeed, $K(\alpha)$ is a subfield of F and it contains K and α, so it contains, by definition $K(\{\alpha\})$. On the other hand, it is clear that $\mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha] \subseteq K(\{\alpha\})$ since they are linear combinations of powers of α with coefficients in K. And since $K(\{\alpha\})$ is a field it contains the inverses of nonzero $K[\alpha]$, that is, it contains $K(\alpha)$.

If the set S is finite, say $S = \{\alpha_1, \ldots, \alpha_n\}$ then we will drop the brackets and simply write $K(\alpha_1, \ldots, \alpha_n)$ instead of $K(\{\alpha_1, \ldots, \alpha_n\})$. Furthermore, we have

$$K(\alpha_1, \cdots, \alpha_n) = K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n).$$

Indeed, $K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$ is, by definition, the smallest field which contains $K(\alpha_1, \cdots, \alpha_{n-1})$ and α_n. This means it contains K and $\alpha_1, \cdots, \alpha_n$, so, by definition

$$K(\alpha_1, \cdots, \alpha_n) \subseteq K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n).$$

For the other inclusion, $K(\alpha_1, \cdots, \alpha_n)$ contains, K and $\alpha_1, \cdots, \alpha_{n-1}$, which means that, by definition

$$K(\alpha_1, \cdots, \alpha_{n-1}) \subseteq K(\alpha_1, \cdots, \alpha_n).$$

And since $\alpha_n \in K(\alpha_1, \cdots, \alpha_n)$, again by definition

$$K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) \subseteq K(\alpha_1, \cdots, \alpha_n).$$

This means that extensions of this kind are simply iterated simple extensions.

2.2 Degree of an extension

2.2.1 Definition and properties

If we have a field extension $K \subseteq F$ then F is a K-vector space. Indeed, the addition is the addition defined on F by virtue of being a field, as is the multiplication by elements of K. All of the vector space axioms follow immediately from the fact that F is a field. This leads to the following definition

Definition 2.2 (Degree of an extension)**.** The *degree* of a field extension $K \subseteq F$ is the dimension of F as a vector space. We write it $[F\colon K]$. An extension of finite degree is called *finite*, otherwise it is called *infinite*. △

Proposition 2.2 (Degree of a simple extension)**.** *If α is algebraic over a field K*[1] *then the degree of the simple extension $K \subseteq K(\alpha)$ is the degree of the minimal polynomial of α over K. That is,*

$$[K(\alpha)\colon K] = \deg(m_{\alpha,K}(x)).$$

Proof. We will show that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $K(\alpha)$, where n is the degree of $m_\alpha(x)$.

Since α is algebraic we know $K[\alpha] = K(\alpha)$. And since $K[\alpha]$ is, by definition, $\mathrm{im}(\mathrm{ev}_\alpha)$ every element of $K(\alpha)$ is a polyomial expression in α with coefficients in K. Say

$$m_\alpha(x) = x^n + \sum_{k=0}^{n-1} a_k x^k.$$

Then, since $m_\alpha(\alpha) = 0$ then

$$\alpha^n = -\sum_{k=0}^{n-1} a_k x^k. \tag{2.2.1}$$

Using eq. (2.2.1) we can rewrite any linear combination of powers of α as a linear combination of powers of α less than n. This means that $1, \alpha, \ldots, \alpha^{n-1}$ span $K(\alpha)$.

Let's now show that they are linearly independent. Say there were $a_0, \ldots a_{n-1} \in K$ such that

$$\sum_{k=0}^{n-1} a_k \alpha^k = 0.$$

This would translate to a polynomial $q(x) = \sum_{k=0}^{n-1} a_k x^k$ that evaluates to 0 at α. Thus it would be divisible by $m_\alpha(x)$, but since $q(x)$ is of degree at most $n-1$ the

[1] α is understood to lie in some extension of K.

only possibility is that $q(x)$ is actually the zero polynomial. That means $a_0 = \cdots = a_{n-1} = 0$, which shows that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent. □

On the other hand, if α is transcendental then $K(\alpha)$ has infinite degree over K. Indeed, since $K(\alpha) \cong K(x)$ it contains a copy of $K[x]$ which has infinite dimension as a K-vector space.

A very similar argument to the proof of proposition 2.2 shows that the degree of an extension of the form $K[x]/\langle p(x)\rangle$ where $p(x)$ is irreducible is $\deg p(x)$. Indeed, extensions of this form are essentially simple extensions constructed without the need for the primitive element to exist in a prior extension, the class of x, $\bar{x}$ plays its role.

Example 2.1. With proposition 2.2 we can calculate the degree of various extensions.

(*i*) We have $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. Indeed, the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ given that it is irreducible over $\mathbb{Q}$ since it has no roots. Similarly, the minimal polynomial of $\sqrt{3}$ is $x^2 - 3$.

(*ii*) Since the complex numbers have dimension 2 as a $\mathbb{R}$-vector space then $[\mathbb{C}\colon \mathbb{R}] = 2$. Another way to show this is by noting that the minimal polynomial of i over $\mathbb{R}$ is $x^2 + 1$ and $\mathbb{C} = \mathbb{R}(i)$. By the same argument, $[\mathbb{Q}(i)\colon \mathbb{Q}] = 2$ since $x^2 + 1$ is also the minimal polynomial of i over $\mathbb{Q}$.

(*iii*) It is known that π and e are transcendental over the rationals, with proofs due to Lindemann and Hermite respectively. This means that both $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are infinite. Consequently, since both extensions are contained within the reals it follows that $\mathbb{R}$ is also infinite over $\mathbb{Q}$.

(*iv*) Let's calculate $[\mathbb{Q}(\sqrt{2} + \sqrt{3})\colon \mathbb{Q}]$. We have

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}.$$

Therefore

$$24 = [(\sqrt{2} + \sqrt{3})^2 - 5]^2 = (\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 25.$$

Thus we have found that $\sqrt{2}+\sqrt{3}$ is a root of $p(x) = x^4 - 10x^2 + 1$. The only possible rational roots of this polynomial are 1 and -1, and it is easily checked that they are not. However this does not prove that $p(x)$ is irreducible, since its degree is higher than 3. However this is a biquadratic polynomial (a polynomial that is quadratic in

x^2), meaning its real roots can be computed, and so it can be factored over $\mathbb{R}$. With this factorisation, one would compute all four possible degree 2 factors of $p(x)$ and find that none of them are rational, thus concluding that $p(x)$ is irreducible over the rationals —if $p(x)$ factored as the product of a degree 3 and a degree 1 polynomial it would have a rational root, which is not the case, so it can only factor as two degree 2 polynomials—. All of this means that

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3})\colon \mathbb{Q}] = 4.$$

$\triangledown$