ALGEBRAIC STRUCTURES 2

Ehud de Shalit

The lecture notes start where we were just before Pesach.
They follow more or less Stewarts's book Galois Theory.

1. Ruler and Compass

1.1. **Geometric constructions with ruler and compass.** Consider a set S of points in the plane (S may be finite or infinite). We are given a compass and an unmarked ruler (so we can draw straight lines but not measure distances). We are allowed to do one of the following:

- draw the line connecting two chosen points of S (extending indefinitely to both sides).
- open the compass to the distance between two given points of S, and draw a circle around a third point (which may be one of the two).

These are the lines and circles *defined by* the set S. We now get new points - intersections of two lines, two circles, or a line and a circle defined by S. Any such new point is said to be *constructible from S in one step*. We add these new points to our set S and repeat the construction based on the larger set of points. Any point P that can be reached in this way after a finite number of steps is said to be *constructible from S*. The question is: which points can we construct in such a way?

For example, if we start with only one point, we can't do anything.

If we start with two points $S = \{A, B\}$ we can construct the line l between them, the circle with radius AB around A and a circle of the same radius around B. The two circles intersect in points P and Q on opposite sides of l. The points P and Q are constructible from S in one step (there are two more such points - which ones?). When we join P and Q by a line m the intersection of l and m gives us a point C which divides AB into equal segments (prove!). We may now continue in this way and get infinitely many new points.

Two famous problems posed by the ancient Greeks were the following:

- *Squaring the circle*: given two points O and A, construct a point B such that the areas of the disk with radius OA and the square with side OB are equal. (It is enough to construct the point B, because highschool geometry tells us how to construct then the desired square).
- *Dividing an angle by three:* given three points O, A, B, find a point C such that

$$\angle AOB = 3\angle AOC. \tag{1.1}$$

Using what we already know about fields we shall show that the first problem is impossible in principle, and that the second one is impossible except if $\angle AOB$ is rather special (for example, $90°$).

Exercise 1.1. *If $\angle AOB = 90°$, describe a construction of a point C such that $\angle AOC = 30°$.*

The *algebraic* proof that certain geometric constructions are impossible was one of the most remarkable successes of algebra in general, and field theory in particular.

1.2. **An algebraic reformulation.** Since S must contain at least two points, we may introduce coordinates in the plane in such a way that $(0,0)$ and $(1,0)$ are among the points in S. Suppose first that P can be constructed from the set S. This means that there exists an increasing sequence of sets

$$S = S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n \tag{1.2}$$

such that $S_i = S_{i-1} \cup \{P_i\}$, P_i is contsructible from S_{i-1} in one step, and $P = P_n$. The *key idea* is to consider the *fields* $K_i = \mathbb{Q}(S_i)$ generated by the x and y-coordinates of all the points in S_i. Thus K_i is a subfield of $\mathbb{R}$ and $K_i = K_{i-1}(x_i, y_i)$ if $P_i = (x_i, y_i)$. [Remark: it is possible to think of points in the plane as complex numbers and consider, instead of the fields K_i, the fields L_i, which are generated inside $\mathbb{C}$ by the numbers in S_i (rather than by their real and imaginary parts). For example $L_i = L_{i-1}(x_i + \sqrt{-1}y_i)$. The arguments below can be modified to deal with the L_i and yield the same results.]

Proposition 1.1. *In the above situation, $K_i = K_{i-1}$ or $[K_i : K_{i-1}] = 2$.*

Proof. The point $P_i = (x_i, y_i)$ is an intersection point of (i) two lines defined by S_{i-1} (ii) a line and a circle defined by S_{i-1}, or (iii) two circles defined by S_{i-1}. Let us treat case (ii). Since the line and the circle are defined by points form S_{i-1} their equations may be written as

$$ax + by = c \tag{1.3}$$

$$(x-p)^2 + (y-q)^2 = m$$

where a, b, c, p, q, m lie in K_{i-1} (you may need to recall your highschool analytic geometry to justify this!). To get x_i eliminate y from the linear equation and substitute in the quadratic equation, getting a quadratic equation for x_i with coefficients from K_{i-1}. Thus $[K_{i-1}(x_i) : K_{i-1}] = 1$ or 2. From the linear equation we see that $K_i = K_{i-1}(x_i, y_i) = K_{i-1}(x_i)$. ∎

Exercise 1.2. *Do cases (i) and (iii). In case (i) show that $K_i = K_{i-1}$. In case (iii) there are two quadratic equations to be solved simultanously. Still, $[K_i : K_{i-1}] \leq 2$. Why?*

Corollary 1.2. *If $P = (x, y)$ can be constructed from a set S of points in the plane, and $K = \mathbb{Q}(S)$, then $[K(x,y) : K]$ is a power of 2.*

Proof. Let $K = K_0 \subset \cdots \subset K_n$ be a sequence of extensions as above such that $x, y \in K_n$. We have seen that each $[K_i : K_{i-1}]$ is either 1 or 2. By the *multiplicativity of degrees in towers* $[K_n : K]$ is a power of 2. Since $K \subset K(x,y) \subset K_n$, $[K(x,y) : K]$ must divide $[K_n : K]$, hence is also a power of 2. ∎

Question: Can you give an example in which $[K(x,y) : K] > 2$? Is $K(x,y)$ necessarily one of the fields K_i?

Discussion. Although we presently only need the corollary, it is interesting to note that it has a converse. The immediate guess, that (x,y) is constructible from S *if and only if* $[K(x,y) : K]$ is a power of 2, turns out to be *false.* However, we have the following:

Theorem 1.3. *The point (x,y) is constructible from S if and only if one can find a sequence of fields*

$$\mathbb{Q}(S) = K \subset K_1 \subset \cdots \subset K_n \tag{1.4}$$

such that K_i/K_{i-1} is a quadratic extension, and $x, y \in K_n$.

We have seen that the condition in the theorem is necessary. To prove that it is sufficient, it is enough to check that if K_1/K is a quadratic extension, then any point whose coordinates lie in K_1 is constructible from S. We can then replace S by a set S_1 all of whose points are constructible from S such that $\mathbb{Q}(S_1) = K_1$ and proceed by induction. Note that the claim is not a-priori obvious even for points with coordinates in K. We have to physically present certain basic geometric constructions that mimic the four operations of algebra *and* the operation of extracting a square root. This is not difficult, and we shall return to it later in the course.

The reason that it is not enough to stipulate that $[K(x,y) : K]$ is a power of 2, is that this does not guarantee that we can "climb" to $K(x,y)$ (or even to a field K_n strictly containing $K(x,y)$) with a tower, each step of which is a quadratic extension. To understand this, however, we shall need the full force of Galois Theory, which is still ahead of us.

1.3. **Squaring the circle.** In this problem $S = \{O = (0,0),\ A = (1,0)\}$ so $K = \mathbb{Q}$. We are required to construct a point $B = (x,y)$ whose distance to the origin is $\sqrt{\pi}$. Copying the segment OB on the line through O and A we may then be able to construct the point $(\sqrt{\pi}, 0)$. It would follow that $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is a power of 2, and in particular finite!

As $\pi \in \mathbb{Q}(\sqrt{\pi})$, it would follow that π is algebraic over $\mathbb{Q}$. This would violate the following famous theorem.

Theorem 1.4. *(Lindemann) The number π is transcendental.*

The proof of Lindemann's theorem is beyond the scope of our course, and uses some analysis. You can find it in Stewart's book in the chapter on Transcendental Numbers. In any case, by the discussion above, it immediately implies that it is impossible to square the circle using compass and ruler only.

1.4. **Trisecting an angle.** In this problem we are given the points

$$S = \{O = (0,0),\ A = (1,0),\ B = (\cos\alpha, \sin\alpha)\}\,. \tag{1.5}$$

Note that A and B lie on the unit circle and $\angle AOB = \alpha$. Here $K = \mathbb{Q}(S) = \mathbb{Q}(\cos\alpha, \sin\alpha)$. We are required to construct $C = (x,y) = (\cos\theta, \sin\theta)$ where $3\theta = \alpha$. We use the elementary identity

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta. \tag{1.6}$$

It follows that

$$4x^3 - 3x - \cos\alpha = 0. \tag{1.7}$$

If this equation is irreducible over $\mathbb{Q}(\cos\alpha)$ then $[\mathbb{Q}(\cos\alpha, x) : \mathbb{Q}(\cos\alpha)] = 3$.

Exercise 1.3. *Prove that this implies also* $[K(x) : K] = 3$. Hint*: K is either equal to $\mathbb{Q}(\cos\alpha)$ or to a quadratic extension of it (why?). In the first case there is nothing to prove. In the second, compute the degree*

$$d = [K(x) : \mathbb{Q}(\cos\alpha)]$$

in two ways; first passing through the intermediate field $\mathbb{Q}(\cos\alpha, x)$, to show that 3 divides d. Then passing through K to show that 3 must divide $[K(x) : K]$.

Proposition 1.5. *If $4x^3 - 3x - \cos\alpha$ is irreducible over $\mathbb{Q}(\cos\alpha)$ then α can not be trisected by ruler and compass.*

Proof. If we could trisect it, we could construct the point C, so $[K(x) : K]$ should have been a power of 2, contradicting the claim in the exercise. ∎

All that remains to be done is to exhibit examples where $4x^3 - 3x - \cos\alpha$ is irreducible over $\mathbb{Q}(\cos\alpha)$. It is simplest to let $\cos\alpha$ be rational. For example, if $\cos\alpha = 1/2$ we get $8x^3 - 6x - 1 = 0$, or, putting $y = 2x$, the equation $y^3 - 3y - 1 = 0$, and finally substituting $y = z + 1$, we get the equation $z^3 + 3z^2 - 3 = 0$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Hence the original equation was irreducible as well.

Note that if $\alpha = 90°$ we get the equation $4x^3 - 3x = x(4x^2 - 3)$ which *is* reducible, in accordance with the fact that a right angle *can* be trisected by ruler and compass.

1.5. **Duplicating the cube.** Another famous theorem along the same lines, which you should now be able to prove for yourself (do it!) is the following.

Proposition 1.6. *Given two points A and B in the plane, it is impossible to construct from them a point C such that the volume of the cube with side AC is twice the volume of the cube with side AB.*

2. The idea behind Galois theory

Galois theory studies finite extensions of fields. We have seen one point of view, which regards the finite extension L of K as a K-vector space of dimension $[L : K]$. This point of view alone was strong enough to yield the results on constructions using ruler and compass, but it does not take into account the rich structure of L as a field. Evariste Galois had the briliant idea to associate to a given finite extension L/K a *group* that, under certain circumstances, tells us much about the extension, for example what are all the subextensions (intermediate fields) and how they sit in each other. It is remarkable to note that at the time of Galois the abstract concept of a group, as you encountered in the first semester, did not exist yet, and that Galois theory was one of the forces that led to the development of group theory.

2.1. **Fields and their automorphism groups.** Let L be a field. Recall that the group of all *automorphisms* of L is

$$Aut(L) = \{\sigma : L \to L | \, \sigma \text{ is an automorphism}\}. \tag{2.1}$$

Thus an element of $Aut(L)$ is a bijective (one-to-one and onto) map σ of L onto itself, that carries 0 to 0, 1 to 1, and respects the field operations: for all x and y in L,

$$\sigma(x+y) = \sigma(x) + \sigma(y), \ \sigma(xy) = \sigma(x)\sigma(y). \tag{2.2}$$

The group law in $Aut(L)$ is *composition:*

$$(\sigma\tau)(x) = \sigma(\tau(x)). \tag{2.3}$$

(You should check at this point that if σ and τ are automorphisms, so is $\sigma\tau$). The identity e of the group $Aut(L)$ is the map $e(x) = x$ (don't confuse it with the constant map sending every x to 1, which is never bijective). The inverse σ^{-1} of σ is the inverse function: $y = \sigma^{-1}(x)$ is the unique element of L for which $\sigma(y) = x$. Check that if σ is an automorphism, so is σ^{-1} !

The group $Aut(L)$ always has at least one element, namely e. An automorphism different from the identity is called *non-trivial.* Sometimes there are no non-trivial automorphisms. In the following exercise the first two examples should be easy. The third might be surprising.

Exercise 2.1. *Prove that L does not have any non-trivial automorphism when L is (a) $\mathbb{Q}$ (b) $\mathbb{F}_p$ (c) $\mathbb{R}$ (note that we are* not *making any assumptions of continuity on our automorphisms).*

Exercise 2.2. *Let $\mathbb{R}(t)$ be the field of rational functions in the variable t over $\mathbb{R}$. Show that if*

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \tag{2.4}$$

($GL_2(\mathbb{R})$ is the group of 2 by 2 invertible matrices over the reals), then there is a unique automorphism σ_g of $\mathbb{R}(t)$ for which $\sigma_g(x) = x$ whenever $x \in \mathbb{R}$ and

$$\sigma_g(t) = \frac{at+b}{ct+d}. \tag{2.5}$$

Compute $\sigma_g\sigma_h$. Can you modify *the definitions so that we shall have $\sigma_g\sigma_h = \sigma_{gh}$?*

Exercise 2.3. *Let L be a field of characteristic p, and $\varphi(x) = x^p$. Prove that φ respects the field operations and that it is injective. Thus it is an automorphism if and only if it is* onto. *In general, φ need not be an automorphism, and is only an endomorphism (a field homomorphism of L into itself), called the* Frobenius endomorphism *or the* Frobenius substitution. *Hint: the only surprising fact is that in characteristic p*

$$(x+y)^p = x^p + y^p. \tag{2.6}$$

Expand using Newton's binomial formula and show that the coefficients $\begin{pmatrix} p \\ i \end{pmatrix}$ $(0 < i < p)$ are divisible by p, hence are 0 in L.

2.2. **The Galois group of an extension.** Now let L/K be an extension of fields (so far assumed arbitrary, not necessarily finite, not necessarily even algebraic). The *Galois group* $Gal(L/K)$ of the extension (we say "Galois L over K") is the subgroup of $Aut(L)$ consisting of all the automorphisms of L which fix K pointwise:

$$Gal(L/K) = \{\sigma \in Aut(L) | \, \sigma(x) = x \text{ for all } x \in K\}. \tag{2.7}$$

Note that this is indeed a *subgroup*. Since the group axioms already hold in $Aut(L)$ we need only check that $Gal(L/K)$ is closed under composition and inverse. For example, if $\sigma(x) = x$ and $\tau(x) = x$ for all $x \in K$, then $\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x$ for all $x \in K$ as well.

Example 2.1. *Let $\rho(z) = \bar{z}$ be complex conjugation. We claim that $Gal(\mathbb{C}/\mathbb{R}) = \{e, \rho\}$. Indeed, ρ is an automorphism fixing the reals pointwise. Conversely, if $\sigma \in Gal(\mathbb{C}/\mathbb{R})$, $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, so $\sigma(i) = \pm i$. For any real x and y*

$$\begin{aligned} \sigma(x+iy) &= \sigma(x) + \sigma(i)\sigma(y) \\ &= x \pm iy \end{aligned} \tag{2.8}$$

since σ fixes the real numbers pointwise. If we take the $+$ sign we get the identity, and if we take the $-$ sign, we get ρ.

Example 2.2. *Let $\zeta = e^{2\pi i/p}$ where p is a prime number, and $L = \mathbb{Q}(\zeta)$. We claim that the irreducible polynomial of ζ over $\mathbb{Q}$ is*

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1. \tag{2.9}$$

First, $\Phi_p(\zeta) = 0$ (ζ annihilates the numerator but not the denominator). Secondly, if we substitute $X = 1 + Y$ we get

$$\begin{aligned} \Phi_p(1+Y) &= \frac{(1+Y)^p - 1}{Y} \\ &= \frac{(Y^p + pY^{p-1} + \cdots + pY + 1) - 1}{Y} \\ &= Y^{p-1} + pY^{p-2} + \cdots + p \end{aligned} \tag{2.10}$$

which is an Eisenstein polynomial (for the prime p), hence is irreducible over $\mathbb{Q}$. It follows that the original polynomial $\Phi_p(X)$ is also irreducible (if $\Phi_p(X) = F(X)G(X)$ is a decomposition into a product of two polynomials, the same would be true for $\Phi_p(1+Y) = F(1+Y)G(1+Y)$).

We have seen that Φ_p (called the cyclotomic polynomial of degree p*) is irreducible, so that*

$$[L : \mathbb{Q}] = \deg \Phi_p = p - 1. \tag{2.11}$$

Moreover, by what we learned in class LIFNEI HAMABUL (I hope you remember...) we have an isomorphism of fields

$$\varphi_1 : \mathbb{Q}[X]/(\Phi_p) \simeq L \tag{2.12}$$

such that $\varphi_1(X \bmod \Phi_p) = \zeta$.

Now if $1 \le a \le p-1$, $\zeta^a = e^{2\pi i a/p}$ is also a primitive pth root of 1, and a root of Φ_p in the field L. So we have a similar isomorphism

$$\varphi_a : \mathbb{Q}[X]/(\Phi_p) \simeq L \tag{2.13}$$

with $\varphi_a(X \bmod \Phi_p) = \zeta^a$. *We now get an* automorphism σ_a *of* L *by setting*

$$\sigma_a = \varphi_a \circ \varphi_1^{-1}. \tag{2.14}$$

Note that we do not have to prove that σ_a *is an automorphism: it is an isomorphism of* L *onto itself because it is the composition of two field isomorphisms. Clearly* $\sigma_a(\zeta) = \zeta^a$.

We claim that

$$Gal(L/\mathbb{Q}) = \{e = \sigma_1, \ldots, \sigma_{p-1}\}. \tag{2.15}$$

Let $\sigma \in Gal(L/\mathbb{Q})$. *Since* $\Phi_p(\sigma(\zeta)) = \sigma(\Phi_p(\zeta)) = 0$, $\sigma(\zeta)$ *is one of the roots of* Φ_p, *some* ζ^a. *Thus* σ *agrees with* σ_a *on* ζ. *But every element of* L *can be written as a polynomial with rational coeficients in* ζ, *and both* σ *and* σ_a *fix* $\mathbb{Q}$, *so if they agree on* ζ, *they agree on all of* L. *It follows that* σ *must be one of the* σ_a.

Exercise 2.4. *Prove that in the previous example* $\sigma_a\sigma_b = \sigma_{ab}$, *so that*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \tag{2.16}$$

as groups.

Example 2.3. *Let* $\alpha^3 = 2$. *We have seen that* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. *Nevertheless,* $G = Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{e\}$. *Indeed, if* $\sigma \in G$, *then* $\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2$, *so* $\sigma(\alpha)$ *should be an element of* $\mathbb{Q}(\alpha)$ *whose cube is 2, but the only such element is* α, *because* $\mathbb{Q}(\alpha) \subset \mathbb{R}$ *and the equation* $x^3 = 2$ *has only one root, namely* α, *in* $\mathbb{R}$ *(the other two roots are complex).*

Example 2.4. *Let* k *be your favorite field in characteristic* p *(mine is* $\mathbb{F}_p$...), $K = k(t)$ *the field of rational functions in the variable* t, *and consider the polynomial*

$$X^p - t \in K[X]. \tag{2.17}$$

It is irreducible over K *by an extension of the Eisenstein criterion from the ring* $\mathbb{Z}$ *to the ring* $k[t]$. *Note that* $k[t]$ *is a* principal ideal domain *(Hug Rashi), and that* t *is a prime element there (why?). Moreover,* K *is the field of fractions of* $k[t]$. *Gauss' Lemma and Eisenstein's irreducibilty criterion are valid there with the same proof as over* $\mathbb{Z}$. *Thus* $X^p - t$ *is an Eisenstein polynomial (for the prime* t*) and is irreducible in* $K[X]$, *just as* $X^p - 5$ *is an Eisenstein polynomial (for the prime* 5*) and is irreducible in* $\mathbb{Q}[X]$. *Don't let the fact that the coefficients in* $X^p - t$ *are themselves polynomials (in* t*) confuse you, and note how the irreducibility (or, equivalently, the primality) of* t *(in* $k[t]$*) is used to deduce the irreducibility of* $X^p - t$ *(in* $K[X]$*).*

Now let $L = K[X]/(X^p - t) = K(x)$ *where* x *is the class of* X, *namely the solution (in* L*) to* $x^p = t$. *Since* $L = K(x) = k(t, x)$ *and* t *is a power of* x, $L = k(x)$. *Since* x *must be transcendental over* k *(if it were algebraic,* t *would be algebraic over* k *too),* L *is again a field of rational functions over* k, *this time in the variable* x. *By what we have learned*

$$[L : K] = \deg(X^p - t) = p. \tag{2.18}$$

We claim that $Gal(L/K) = \{e\}$. *For that note that if* y *is any solution in* L *to* $X^p = t$ *then*

$$(y - x)^p = y^p - x^p = t - t = 0. \tag{2.19}$$

It follows that $y = x$. *Now any* $\sigma \in Gal(L/K)$ *must satisfy* $\sigma(x)^p = \sigma(x^p) = \sigma(t) = t$, *so* $\sigma(x) = x$. *As* σ *fixes* K *pointwise, it must fix* $L = K(x)$, *and* $\sigma = e$.

Example 2.5. *It can be shown that all the automorphisms of* $\mathbb{R}(t)$ *over* $\mathbb{R}$ *are of the form* σ_g *for* $g \in GL_2(\mathbb{R})$.

2.3. **Discussion of the examples.** The five examples above are typical of what happens. The last one is a transcendental extension. While Galois theory for transcendental extensions is interesting, it will not be covered in this course, and you may forget about this example. The first four examples are algebraic, and even *finite* (remember that an algebraic extension is finite if and only if it is finitely generated - in all these examples L was in fact a *simple* extension of K, generated by one element).

In the first two examples, $|Gal(L/K)| = [L : K]$. We shall show later that the Galois group of a finite extension is always finite and

$$|Gal(L/K)| \leq [L : K]. \tag{2.20}$$

When equality holds, we say that L/K is a *Galois extension.* We shall also show that L/K is a Galois extension if and only if it satisfies two conditions, called *normality and separability.*

Normality means "*one root in, all roots in*": if an *irreducible* polynomial over K acquires one root in L, it must acquire all its roots in L, hence split into a product of linear factors over L. The third example is not normal. The irreducible polynomial $X^3 - 2$ (over $\mathbb{Q}$) acquires over L one root only and decomposes into the product of $(X - \alpha)$ with a quadratic polynomial. Lack of normality can be remedied by going to a larger extension (in this example an extension of degree 2 of L, and altogether of degree 6 of $\mathbb{Q}$), in which the given polynomial splits completely. More precisely, we shall show that any finite extension can be embedded in a larger finite extension which is normal.

Separability means that irreducible polynomials over K factor over L into relatively prime factors. The fourth example is non-separable: the irreducible polynomial $X^p - t$ factors over L as $(X - x)^p$. Separability can not be remedied by going to a larger extension. If $X^p - t$ factored over L into a product of p identical linear factors, then this same factorization will remain valid over any larger field.

Luckily, we shall see that in characteristic 0 every finite extension is separable. Inseparability may occur only in characteristic p.

2.4. **The Galois correspondence.** If L/K is a finite extension which is *Galois* (equivalently, normal and separable) then the main theorem of Galois theory will give an *inclusion-reversing bijection* between *intermediate fields* M

$$K \subset M \subset L \tag{2.21}$$

and *subgroups* $G \supset H \supset \{e\}$ of $G = Gal(L/K)$. The bijection $M \leftrightarrow H$ is given by the rule

$$\begin{aligned} H &= Gal(L/M), \\ M &= \text{field of elements fixed by } H. \end{aligned} \tag{2.22}$$

If we know G we can determine the Boolean structure of the subfields of L containing K completely: namely we can list them, and tell which contains which. The bijection, called the *Galois correspondence,* is explicit enough to allow computations, such as of generators of M, in given examples. It also allows us to say when M/K would be normal (if an only if the corresponding subgroup H is normal in the

sense of group theory). In such a case M/K would be Galois (separability, unlike normality, is inherited by M from L) and we would have $Gal(M/K) \simeq G/H$.

The Galois correspondence itself can be *defined* for *any* extension L/K, and its first properties are very easy to establish, even if they do not yield a bijection between subgroups and subfields. We shall do it now, and in the next section study in detail the two properties of normailty and separability. We shall then deduce the Main Theorem of Galois theory and see some examples. This is the plan for the next 3 weeks.

Definition 2.1. *Let L/K be an extension of fields, and $G = Gal(L/K)$. For any subgroup H of G we let*

$$\mathcal{F}(H) = \{x \in L | \, \sigma(x) = x \text{ for every } \sigma \in H\}. \tag{2.23}$$

and for every field $K \subset M \subset L$ we let

$$\mathcal{G}(M) = Gal(L/M). \tag{2.24}$$

Proposition 2.1. *(i) $\mathcal{F}(H)$ is an intermediate field $K \subset \mathcal{F}(H) \subset L$.*
(ii) $\mathcal{F}(\{e\}) = L$.
(iii) If $H_1 \supset H_2$ then $\mathcal{F}(H_1) \subset \mathcal{F}(H_2)$.

Proof. (i) Clearly $\mathcal{F}(H)$ contains K because every σ leaves K fixed pointwise. If $\sigma(x) = x$ and $\sigma(y) = y$ then $\sigma(x \pm y) = x \pm y$, $\sigma(xy) = xy$ and $\sigma(x^{-1}) = x^{-1}$, so $\mathcal{F}(H)$ is a subfield of L. Note that in proving part (i) we did not use the fact that H was a subgroup of G. It could be any *subset* of G and still $\mathcal{F}(H)$ would be a subfield of L containing K.

(ii) This is clear.

(iii) If we relax the conditions, we get a larger set: elements of $\mathcal{F}(H_1)$ are fixed by every $\sigma \in H_1$, hence clearly by every $\sigma \in H_2$. ∎

Proposition 2.2. *(i) $\mathcal{G}(M)$ is a subgroup of G.*
(ii) $\mathcal{G}(L) = \{e\}$, $\mathcal{G}(K) = G$.
(iii) If $M_1 \subset M_2$ then $\mathcal{G}(M_1) \supset \mathcal{G}(M_2)$.

Proof. The proofs are mirror images of the proofs of the previous proposition and we leave them as an exercise. Note that if σ is an automorphism of L fixing M pointwise, then it clearly fixes pointwise the smaller set K, hence belongs to G. Note that here too, point (i) does not rely on M being a subfield. It can be any subset containing K. ∎

Despite the similarity between the two propositions, there is a lack of symmetry regarding point (ii). In the first proposition we *did not claim* that $\mathcal{F}(G) = K$. This will turn out to be equivalent to L/K being Galois!

Proposition 2.3. *For any intermediate field M, $M \subset \mathcal{F}(\mathcal{G}(M))$. For any subgroup H, $\mathcal{G}(\mathcal{F}(H)) \supset H$.*

Proof. Every element of M is fixed by any element of G that fixes every element of M. Conversely, every element of H fixes any element of L that is fixed by all the elements of H. ∎

Exercise 2.5. *Prove that $\mathcal{G}(\mathcal{F}(\mathcal{G}(M))) = \mathcal{G}(M)$, and that $\mathcal{F}(\mathcal{G}(\mathcal{F}(H))) = \mathcal{F}(H)$. (Hint: for the second identity, for example, take in the first inclusion of the proposition $M = \mathcal{F}(H)$, and to the second* apply *$\mathcal{F}$.)*

The field $\mathcal{F}(H)$ is called the *fixed field of* H. It is sometimes denoted L^H. The group $\mathcal{G}(M)$ needs no new name: it is the *Galois group of* L *over* M.

3. Normality and Separability

3.1. **Splitting fields.** We recall things that we did before the break. Let K be a field and $f \in K[X]$, $\deg(f) = n$. We say that f *splits over* K if

$$f = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n). \tag{3.1}$$

If f is monic, $c = 1$. The roots $\alpha_1, \dots, \alpha_n$ need not be distinct, but if f has n distinct roots in K it clearly splits there.

We call an extension L/K a *splitting field* for f if (i) f splits over L (ii) if $L' \subset L$ and F already splits over L', then $L' = L$. Sometimes, to emphasize (ii) people say that L is a *minimal* splitting field for f, but our convention will be that a "splitting field" is already a minimal one. If f splits over L and α_i are its roots (as above, maybe with repetitions), the minimal subfield of L over which it splits is $K(\alpha_1, \dots, \alpha_n)$. It follows that L is a splitting field if and only if f splits over it, and L is already generated over K by the α_i.

Theorem 3.1. *Any* $f \in K[X]$ *has a splitting field* L*, and if* $\deg(f) = n$*, then* $[L : K] \leq n!$

Proof. By induction on n. If $n = 1$, then $f = c(X - \alpha)$ and $L = K$. Now let g be an irreducible factor of f, so that $f = gh$. We have seen that in the field

$$M = K[X]/(g) \tag{3.2}$$

the element $\alpha_1 = X \bmod (g)$ is a root of g, hence of f. Furthermore $M = K(\alpha_1)$ and

$$[M : K] = \deg(g) \leq n. \tag{3.3}$$

Over M

$$f = (X - \alpha_1)f_1 \tag{3.4}$$

and $\deg(f_1) = n - 1$. By induction f_1 has a splitting field $L = M(\alpha_2, \dots, \alpha_n)$ over which

$$f_1 = c(X - \alpha_2)\dots(X - \alpha_n), \tag{3.5}$$

and $[L : M] \leq (n - 1)!$. We conclude that L is a splitting field for f and

$$[L : K] = [M : K][L : M] \leq n(n - 1)! = n! \tag{3.6}$$

∎

The question arises whether the splitting field is unique (up to isomorphism), because we may adjoin the roots in different orders.

Recall the following lemma on extensions of homomorphisms.

Lemma 3.2. *Let* $i : K \to \Omega$ *be an embedding of fields. Let* $L = K(\alpha)$ *be a simple algebraic extension and* $f \in K[X]$ *the minimal polynomial of* α *over* K*. Suppose that* $i(f)$ *has a root* $\tilde{\alpha}$ *in* Ω*. Then there exists a unique homomorphism*

$$j : L \to \Omega \tag{3.7}$$

such that $j|_K = i$ *and* $j(\alpha) = \tilde{\alpha}$.

Proof. Define a ring homomorphism

$$\varphi : K[X] \to \Omega \tag{3.8}$$

by the formula

$$\varphi(\sum a_k X^k) = \sum i(a_k)\tilde{\alpha}^k. \tag{3.9}$$

In other words, on the scalars K we let $\varphi = i$ and $\varphi(X) = \tilde{\alpha}$. We check

$$\varphi(f) = i(f)(\tilde{\alpha}) = 0, \tag{3.10}$$

so $\ker(\varphi) \supset (f)$. Since f is irreducible, (f) is a maximal ideal, and $\ker(\varphi) = (f)$. It follows that φ induces a field homomorphism

$$\bar{\varphi} : K[X]/(f) \to \Omega \tag{3.11}$$

which coincides with i on K and sends $X \bmod(f)$ to $\tilde{\alpha}$. We also know that there exists an *isomorphism*

$$\bar{\psi} : K[X]/(f) \simeq L \tag{3.12}$$

which is the identity on K and sends $X \bmod(f)$ to α. If we let

$$j = \bar{\varphi} \circ \bar{\psi}^{-1} \tag{3.13}$$

we are done. The uniqueness is clear because if we specify j on K and on α, we specify it completely on $K(\alpha) = L$. ∎

Corollary 3.3. *Let $i : K \to \Omega$ be an embedding of fields, $f \in K[X]$, and L a splitting field of f. Assume that $i(f)$ splits in Ω. Then there is an embedding $j : L \to \Omega$ such that $j|_K = i$ (we say that j* extends *i).*

Proof. By induction on $n = \deg(f)$. If $n = 1$, $L = K$ and $j = i$. In general let α_1 be a root of f in L and f_1 the minimal polynomial of α_1 over K. Since f_1 divides f, $i(f_1)$ splits in Ω, and in particular has a root $\tilde{\alpha}_1$ there. It follows from the lemma that i has an extension $i_1 : L_1 \to \Omega$, where $L_1 = K(\alpha_1)$, and $i_1(\alpha_1) = \tilde{\alpha}_1$. Now replace K by L_1, i by i_1 and f by $g = f/(X - \alpha_1)$. Then L is the splitting field of g over L_1 and $i(g)$ splits completely in Ω because it divides $i(f)$. Since $\deg(g) = \deg(f) - 1$, the induction hypothesis holds (with L_1 as the base field) and we can extend i_1 to an embedding $j : L \to \Omega$. ∎

Theorem 3.4. *Let $i : K \simeq \tilde{K}$ be an isomorphism, $f \in K[X]$ and $\tilde{f} = i(f) \in \tilde{K}[X]$. Let L be a splitting field of f and $\tilde{L}$ a splitting field of $\tilde{K}$. Then there exists an extension of i to an isomorphism j of L onto $\tilde{L}$.*

Proof. If we take $\Omega = \tilde{L}$, then i is an embedding of K in $\tilde{L}$, and $i(f)$ splits in Ω. The corollary implies that we can extend i to $j : L \to \tilde{L}$. But since f splits over L, $i(f)$ splits already over $j(L)$, so by the minimality of $\tilde{L}$, $\tilde{L} = j(L)$, and j is an isomorphism. ∎

Example 3.1. *Consider the polynomial $X^3 - 2$, $\alpha_1 = 2^{1/3}$ (the real root), $\omega = e^{2\pi i/3}$, $\alpha_2 = \omega\alpha_1$ and $\alpha_3 = \omega^2\alpha_1$. Then a splitting field for $X^3 - 2$ over $\mathbb{Q}$ is the subfield of $\mathbb{C}$ given by*

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \omega). \tag{3.14}$$

Note that $[L : \mathbb{Q}(\alpha_1)] = 2$ since $L = \mathbb{Q}(\alpha_1)(\omega)$ and the minimal polynomial of ω over $\mathbb{Q}(\alpha_1)$ is $X^2 + X + 1$.

Exercise 3.1. *Write the decomposition of* $X^3 - 2$ *in* $\mathbb{Q}(\alpha_1)[X]$.

The same field can be obtained as the splitting field of many different polynomials. In the last example L is also the splitting field of $X^3 - 3X^2 + 3X - 3 = (X-1)^3 - 2$, whose roots are the $1 + \alpha_i$.

Lemma 3.5. *Let* L *be a splitting field of some polynomial* g *over* K. *Let* Ω *be an extension of* L *and* $\sigma \in Gal(\Omega/K)$. *Then* $\sigma(L) = L$.

Proof. Write $g = \prod_{i=1}^{r}(X - \alpha_i)$ in L. Then

$$g = \sigma(g) = \prod (X - \sigma\alpha_i). \tag{3.15}$$

By unique factorization, σ must induce a permutation of the α_i. But $L = K(\alpha_1, \dots, \alpha_r)$, so $\sigma(L) = L$. ∎

3.2. **Normal extensions.** An extension L of K is called *normal* if for any irreducible polynomial $f \in K[x]$, if f has a root in L, f splits in L.

Proposition 3.6. *Let* L *be a finite extension of* K. *Then* L *is normal over* K *if and only if it is a splitting field of some polynomial.*

Proof. Suppose L is normal over K and write $L = K(\theta_1, \dots, \theta_m)$. Let g_i be the minimal polynomial of θ_i over K. Since g_i is irreducible and obtains one root in L, it already splits there. Therefore $g = \prod g_i$ splits in L. But the roots of g already generate L over K, since they include the θ_i. It follows that L is the splitting field of g.

Conversely, suppose that L is the splitting field of a polynomial g. Let f be any irreducible polynomial in $K[x]$, and let Ω be the splitting field of f over L. Then Ω is the splitting field of fg over K. Let α and β be two roots of f in Ω. Then there exists an isomorphism

$$\sigma : K(\alpha) \simeq K(\beta) \tag{3.16}$$

which is the identity on K and which carries α to β. Since $\sigma(fg) = fg$, σ can be extended to an automorphism of Ω, which we still denote by the letter σ (Theorem 3.4). By Lemma 3.5, $\sigma(L) = L$. It follows that if $\alpha \in L$, $\beta \in L$ too. Hence if f has a root in L, all its roots lie in L, and it splits. Since this is true for any irreducible $f \in K[x]$, L is a normal extension of K. ∎

The property of being normal is inherited under extension of the *base*. More precisely:

Proposition 3.7. *Let* $L \supset M \supset K$ *be a tower of fields,* $[L : K] < \infty$, *and assume that* L *is normal over* K. *Then* L *is normal over* M *as well.*

Proof. If L is normal over K, it is the splitting field of some $g \in K[x]$ over K. *A fortiori* it is the splitting field of the same polynomial over M. ∎

Exercise 3.2. *Let* L *be a finite normal extension of* K, *and* K' *any extension of* K. *Let* L' *be a field containing both* K' *and* L *and generated by them. Such a field is called a* compositum *of* K' *and* L. *Then* L' *is a normal extension of* K'.

3.3. **Separable polynomials and differentiation.** For a polynomial $f \in K[X]$ we denote by f' the formal derivative of f. If

$$f = \sum a_k X^k \tag{3.17}$$

then

$$f' = \sum k a_k X^{k-1}. \tag{3.18}$$

If $char(K) = 0$, then

$$\deg(f') = \deg(f) - 1. \tag{3.19}$$

However, if $char.K = p$, funny things may happen. For example, the polynomial $X^p - a$ ($a \in K$) has 0 derivative, since $p = 0$ in the field. In general, even if the derivative does not vanish, its degree may be strictly smaller than $\deg(f) - 1$.

Recall that for $f, g \in K[x]$, we denoted by (f, g) their g.c.d., which is obtained via the Euclidean algorithm. The g.c.d. is the same, whether we view the polynomials over K or over a larger field L, because the Euclidean algorithm is the same, irrespective of where we perform it.

We shall be interested in the g.c.d. of f and it derivative f'.

A polynomial f is called *separable* if in a splitting field, all its roots are distinct:

$$f = c\prod_{i=1}^{n}(X - \alpha_i) \tag{3.20}$$

and $\alpha_i \neq \alpha_j$ for $i \neq j$. This notion is independent of the splitting field, because any two splitting fields are isomorphic. The following proposition tells us that to check whether f is separable we do not have to find the roots, or to go to an extension over which f splits. It is enough to carry out the Euclidean algorithm on f and f', inside $K[x]$.

Proposition 3.8. *The polynomial f is separable if and only if $(f, f') = 1$.*

Proof. Let L be a splitting field of f and write

$$f = c\prod_{i=1}^{r}(X - \alpha_i)^{e_i} \tag{3.21}$$

where now the $\alpha_i \in L$ are distinct, and $e_i \geq 1$ (the e_i are called the *multiplicities* of the roots). Clearly

$$f' = c\sum_{i=1}^{r}\left(e_i(X - \alpha_i)^{e_i - 1}\prod_{j \neq i}(X - \alpha_j)^{e_j}\right). \tag{3.22}$$

If some $e_i > 1$, then each term is divisible by $(X - \alpha_i)$, and $(X - \alpha_i)$ divides (f, f') (in $L[x]$), so $(f, f') \neq 1$. If on the other hand f is separable, every $e_i = 1$, then $(X - \alpha_i)$ divides all the summands except for the ith one, and does not divide the ith summand, so $(X - \alpha_i)$ does not divide f'. Since this is true for any of the prime factors of f, the g.c.d. of f and f' is 1. ∎

Exercise 3.3. *Using the above notation, prove that if $char.K = 0$ then*

$$(f, f') = \prod_{i=1}^{r}(X - \alpha_i)^{e_i - 1}. \tag{3.23}$$

What gores wrong in characteristic p?

Corollary 3.9. *If $char(K) = 0$, every irreducible polynomial over K is separable.*

Proof. If $\deg(f) = n$ then $\deg(f') = n - 1$, so (f, f') must be a proper divisor of f. If f is irreducible, it must be 1. ∎

Example 3.2. *Let $K = \mathbb{F}_p(t)$ and $f = X^p - t \in K[X]$. We have seen that f is irreducible, but if x is a root in a splitting field, then*

$$f = X^p - x^p = (X - x)^p \tag{3.24}$$

is not separable. One can not eliminate the condition that char.$(K) = 0$!

3.4. **Separable extensions.** Let L be an algebraic extension of K. An element $\alpha \in L$ is called separable if its minimal polynomial over K is separable. The extension is called separable if all its elements are.

For example, every element of K is separable over K. In characteristic 0 all extensions are separable.

Exercise 3.4. *Let char.$K = p$. Show that if $[L : K]$ is prime to p, then L is a separable extension of K.*

Proposition 3.10. *If $L \supset M \supset K$ and L is separable over K, then both L/M and M/K are separable.*

Proof. For M/K this is obviuos: we only have to check the separability of fewer elements. For L/M let $\alpha \in L$. Its minimal polynomial g_α over M divides the minimal polynomial f_α of the same element over K. But f_α is separable, hence g_α is separable too. ∎

Exercise 3.5. *Let L/K be a separable extension and K'/K an arbitrary extension. Let $L' = LK'$ be a compositum of L and K'. Then $L'/K/$ is also separable.*

4. Field degrees and Group orders

This section covers chapters 9 *and* 10 of Stewart's book,
but in a different order, and the proofs are somewhat different.

4.1. **Galois extensions.** Let L be a finite extension of K and $G = Gal(L/K)$.

Theorem 4.1. *We always have*

$$|G| \leq [L : K], \tag{4.1}$$

and equality holds if and only if L/K is normal and separable.

Lemma 4.2. *Let $L = K(\alpha)$ and let $\sigma : K \to \Omega$ be an embedding. Let f be the minimal polynomial of α over K and σf its image under σ. Then the extensions of σ to an embedding $\tilde{\sigma} : L \to \Omega$ are in 1-1 correspondence with the roots of σf in Ω.*

Proof. We have already seen this before Pesach, but because of its importance, I repeat the proof. We have seen in Lemma 3.2 that for any root $\tilde{\alpha}$ of σf in Ω there exists a unique extension $\tilde{\sigma}$ of σ to L carrying α to $\tilde{\alpha}$ (we denoted there σ and $\tilde{\sigma}$ by i and j, otherwise it's the same claim). On the other hand if $\tilde{\sigma}$ is *any* extension of σ,

$$0 = \tilde{\sigma}(f(\alpha)) = (\sigma f)(\tilde{\sigma}\alpha) \tag{4.2}$$

so $\tilde{\sigma}\alpha$ must be a root of σf. Thus the extensions correspond bijectively to the roots of σf in Ω. ∎

Corollary 4.3. *The number of extensions of a given σ to an embedding of L in Ω is at most $[L:K]$ and it is equal to $[L:K]$ if and only if α is separable over K and σf splits in Ω.*

Proof. If either α is inseparable over K, or if it is separable but σf does not split in Ω, then the number of distinct roots of σf in Ω is strictly less than $\deg(f) = [L:K]$. On the other hand if α is separable *and* σf splits in Ω, then there are precisley $\deg(f)$ distinct roots. ∎

Proof. (of the theorem) Write $L = K(\alpha_1, \ldots, \alpha_r)$ and let $L_0 = K$,

$$L_i = K(\alpha_1, \ldots, \alpha_i). \tag{4.3}$$

We take in the lemma $\Omega = L$ and consider an automorphism of L as built in layers: we start with the identity (inclusion) of $L_0 = K$ into L, and extend it successively form an embedding of L_{i-1} to an embedding of L_i. Since $L_i = L_{i-1}(\alpha_i)$ is a simple extension of L_{i-1}, each embedding of L_{i-1} has at most $[L_i : L_{i-1}]$ extensions to L_i. Altogether the number of embeddings of L in L extending the identity of K is therefore at most

$$[L_1 : L_0][L_2 : L_1] \ldots [L_r : L_{r-1}] = [L : K]. \tag{4.4}$$

It only remains to remark that an embedding of L in itself is an automorphism, since (being an injective linear transformation of a finite dimensional vector space) it is also surjective.

If L is a *separable* and *normal* extension of K, then at each step α_i is separable over K, hence separable over L_{i-1}. Let $g_i \in L_{i-1}[X]$ be the minimal polynomial of α_i over L_{i-1} and $f_i \in K[X]$ its minimal polynomial over K. Then f_i is an irreducible polynomial in $K[X]$, and since it has one root in L, it splits there. Let σ_{i-1} be an embedding of L_{i-1} into L (over K). From

$$g_i | f_i \tag{4.5}$$

we get also

$$\sigma_{i-1}(g_i) | f_i \tag{4.6}$$

(note that $\sigma_{i-1}(f_i) = f_i$). It follows that $\sigma_{i-1}(g_i)$ splits into distinct linear factors over L, so σ_{i-1} has *precisely* $[L_i : L_{i-1}]$ extensions to L_i. The total number of embeddings of L in L extending the identity on K is therefore $[L:K]$.

If on the other hand there was an element $\alpha \in L$ which was either inseparable, or its minimal polynomial did not split in L, we can take $\alpha = \alpha_1$ (we are free to choose any number of generators as we wish, then complete them to a set of generators). It then follows that the number of extensions of the identity from K to $L_1 = K(\alpha_1)$ is strictly less than $[L_1 : K]$ and the arguments above show that $|G|$ is then strictly less than $[L:K]$. ∎

A finite extension in which $|Gal(L/K)| = [L:K]$ is called *Galois.* We proved

Galois = normal + separable.

Some authors reserve the name *Galois group* for $Gal(L/K)$ only when L/K is Galois, and otherwise call it simply the group of automorphisms of L over K.

We shall stick to our convention of calling it the Galois group always, even if the extension of non Galois.

Corollary 4.4. *(i) If $L \supset M \supset K$ is a tower of finite extensions, and L/K is Galois, so is L/M.*

(ii) If K' is an arbitrary extension of K, and $L' = LK'$ a compositum, then if L/K is Galois, so is L'/K'.

Proof. We have seen that normality and separability are inherited in these situations. On the other hand, note that in (i), M/K will not be Galois in general, because it may not be normal. ∎

Exercise 4.1. *A finite extension is Galois if and only if it is the splitting field of a separable polynomial.*

4.2. **Fixed fields and group orders.** So far we have constructed our field extension "bottom up": we started with K, found an extension L, and asked how big $Gal(L/K)$ was. We are now going to reverse the process. We start with a field L and a *finite group* $G \subset Aut(L)$ of automorphisms of L. We let

$$K = \mathcal{F}(G) \tag{4.7}$$

be the fixed field of G, namely the field of elements from L that are fixed pointwise by every $\sigma \in G$. The following inequality goes in a direction *opposite* to the inequality proved in Theorem 4.1

Proposition 4.5. *We have $[L : K] \leq |G|$.*

Proof. Let $G = \{\sigma_1, \ldots, \sigma_m\}$ and suppose that $[L : K] > m$, so there are $\omega_1, \ldots, \omega_n$ in L which are linearly independent over K and $n > m$ (we do not know yet that L/K is finite - this will only follow from the proof). In the matrix

$$(\sigma_i \omega_j)_{1 \leq i \leq m, 1 \leq j \leq n} \tag{4.8}$$

the columns must be linearly dependent over L. Let r be the minimal number of columns between which we can find a linear dependence. Changing the order of the ω_j we may assume that the first r columns are dependent, but every $r-1$ among them are independent. Let

$$\sum_{j=1}^{r} c_j \cdot \sigma_i \omega_j = 0 \tag{4.9}$$

be the linear dependence ($1 \leq i \leq m$) where a-priori $c_j \in L$. Since all the $c_j \neq 0$ we may divide by c_1 and assume $c_1 = 1$. We shall show that in fact $c_j \in K$. To that end, let $\sigma \in G$ be arbitrary and apply it to the linear dependence to get

$$\sum_{j=1}^{r} \sigma c_j \cdot \sigma \sigma_i \omega_j = 0. \tag{4.10}$$

Now when σ_i runs over G, $\sigma\sigma_i$ runs over the same elements in a different order. Re-ordering the equations we get

$$\sum_{j=1}^{r} \sigma c_j \cdot \sigma_i \omega_j = 0. \tag{4.11}$$

Subtracting the original linear dependence from this one we get

$$\sum_{j=2}^{r}(\sigma c_j - c_j)\cdot \sigma_i\omega_j = 0. \tag{4.12}$$

Note that we started the summation from $j=2$, since for $j=1$, $\sigma c_1 - c_1 = 0$. By the minimality of r, all the coefficients in this dependence must vanish, so $\sigma c_j = c_j$. This holds for every $\sigma \in G$, so $c_j \in \mathcal{F}(G) = K$.

Returning to the original linear dependence, and working with any σ_i, we may write it now as

$$\sigma_i(\sum_{j=1}^{r} c_j \cdot \omega_j) = 0. \tag{4.13}$$

This means that $\sum c_j\omega_j = 0$, contradicting the linear independence of the ω_j over K. This contradiction concludes the proof that $[L:K] \leq |G|$. ∎

Theorem 4.6. *Let L be a field, and G a finite group of automorphisms of L. Let $K = \mathcal{F}(G)$ be its fixed subfield. Then L is a Galois extension of K, $G = Gal(L/K)$ and $|G| = [L:K]$.*

Proof. From the proposition, L/K is finite. Clearly $G \subset Gal(L/K)$ because the elements of G fix K pointwise. Theorem 4.1 and Proposition 4.5 give the two inequalities

$$|Gal(L/K)| \leq [L:K] \leq |G|. \tag{4.14}$$

It follows that both inequalities must be equalities, and that $G = Gal(L/K)$. ∎

5. The main theorem of Galois theory

5.1. **The theorem.** We are ready to state and prove the main theorem on the Galois correspondence.

Theorem 5.1. *Let L/K be a finite Galois extension, and $G = Gal(L/K)$. Then the correspondences $\mathcal{F}$ and $\mathcal{G}$ are inverse to each other:*

$$\mathcal{F}\mathcal{G}(M) = M \tag{5.1}$$

for any intermediate field M, and

$$\mathcal{G}\mathcal{F}(H) = H \tag{5.2}$$

for any subgroup H. They therefore set the family of all intermediate fields in bijection with the family of all subgroups of G. Moreover, for any $H \subset G$

$$[L:\mathcal{F}(H)] = |H| \tag{5.3}$$

and for every $L \supset M \supset K$

$$[L:M] = |\mathcal{G}(M)|. \tag{5.4}$$

Proof. The idea is to prove *first* the two numerical equalities. However, the first follows from Theorem 4.6 (applied to H instead of G) and the second follows from Corollary 4.4, since L/M is Galois as well, and $\mathcal{G}(M) = Gal(L/M)$.

We have seen that $\mathcal{F}\mathcal{G}(M) \supset M$. But form the numerical equalities

$$[L:\mathcal{F}\mathcal{G}(M)] = |\mathcal{G}(M)| = [L:M]. \tag{5.5}$$

Since $[L : M] = [L : \mathcal{FG}(M)][\mathcal{FG}(M) : M]$ we deduce that $[\mathcal{FG}(M) : M] = 1$, or that $\mathcal{FG}(M) = M$.

Similarly $\mathcal{GF}(H) \supset H$. From the numerical equalities

$$|\mathcal{GF}(H)| = [L : \mathcal{F}(H)] = |H| \tag{5.6}$$

so $\mathcal{GF}(H) = H$. ∎

What the theorem says is that the only elements of L fixed by all the automorphisms fixing a subfield M, are the elements already in M. Likewise, the only automorphisms fixing every element of the fixed field of a subgroup H are those already in H.

Since $|G| = |H|[G : H]$ we may rewrite the numerical equalities as

$$[\mathcal{F}(H) : K] = [G : H] \tag{5.7}$$

and

$$[M : K] = [G : \mathcal{G}(M)]. \tag{5.8}$$

Don't let the dual usage of the notation $[X : Y]$ confuse you: when these are groups, it is the subgroup index. When these are fields, it is the dimension of the bigger field as a vector space over the base field. In retrospect, the Galois correspondence is the typographical *reason* mathematicians have chosen the same notation for both!

5.2. **Normal subgroups and normal extensions.** We have seen that if M is an intermediate field of a Galois extension L/K with Galois group $G = Gal(L/K)$, then L/M is also Galois. Let $H = Gal(L/M)$ be the corresponding subgroup of G. The following theorem answers the question: *when is M/K Galois?*

Theorem 5.2. *In the above situation, M/K is Galois if and only if H is normal in G, and if this holds there is a canonical identification*

$$Gal(M/K) \simeq G/H. \tag{5.9}$$

Lemma 5.3. *Let L/K be any extension, and $G = Gal(L/K)$. For any subgroup H of G and any $\sigma \in G$*

$$\mathcal{F}(\sigma H \sigma^{-1}) = \sigma \mathcal{F}(H). \tag{5.10}$$

Proof. Let $x \in L$. Then $\sigma h \sigma^{-1}(x) = x$ for every $h \in H$ if and only if $h\sigma^{-1}(x) = \sigma^{-1}(x)$ for every $h \in H$. But this is equivalent to $\sigma^{-1}(x) \in \mathcal{F}(H)$, or $x \in \sigma\mathcal{F}(H)$. ∎

Proof. (of the theorem) We first remark that M/K is Galois if and only if it is normal, because we have already seen that it is separable. If M/K is normal, we have seen in Lemma 3.5 that $\sigma M = M$ for every $\sigma \in G$. If, on the other hand, it is not normal, let $\alpha \in M$ be an element whose minimal polynomial does not split in M. Since it splits in L, there is a root β in L, $\beta \notin M$. The isomorphism of $K(\alpha)$ onto $K(\beta)$ which is the identity on K and which is taking α to β, can be extended to an automorphism $\sigma \in Gal(L/K)$. Then $\sigma M \neq M$ because $\beta = \sigma\alpha \notin M$. Thus $\sigma M = M$ for every $\sigma \in G$ is a *necessary and sufficient* condition for M/K to be normal.

The theorem now follows from the bijectivity of the Galois correspondence: H is normal if and only if $\sigma H \sigma^{-1} = H$ for every $\sigma \in G$. The lemma (and the bijectivity of the Galois correspondence) implies that this is so if and only if $\sigma M = M$ for every σ, which means that M is normal.

Suppose this is the case. Since $\sigma \in G$ maps M to itself, we may define a map

$$G \to Gal(M/K) \tag{5.11}$$

which maps $\sigma \mapsto \bar{\sigma} = \sigma|_M$. It is a group homomorphism whose kernel is precisely H (the automorphisms of L whose restriction to M is the identity of M). We therefore get an injection

$$G/H \hookrightarrow Gal(M/K). \tag{5.12}$$

Since $[M : K] = [G : H]$ (or alternatively, since any automorphism of M can be extended to an automorphism of L), this is an isomorphism. ∎

Exercise 5.1. *A Galois extension is called* abelian *if its Galois group is abelian. Prove that if L/K is a finite abelian extension, then all intermediate fields M are also Galois and abelian over K.*

6. Examples and complements

6.1. **First example.** Let $F = \mathbb{Q}(\alpha)$ where α is the real root of

$$X^3 - 2. \tag{6.1}$$

This is a cubic extension of $\mathbb{Q}$ ($[F : \mathbb{Q}] = 3$) since the polynomial is irreducible (either because it is Eisenstein or simply because it has no root in $\mathbb{Q}$: a polynomial of degree 3 can factor only if it has a root in the field!). The other two roots of the polynomial, $\omega\alpha$ and $\omega^2\alpha$ where $\omega = \exp(2\pi i/3)$ are complex, and in particular not in F. So F is not normal over $\mathbb{Q}$.

Let L be the splitting field of $X^3 - 2$, namely the field generated over $\mathbb{Q}$ by the three roots. It can also be generated by α and ω (why?)

$$L = \mathbb{Q}(\alpha, \omega). \tag{6.2}$$

The cubic root of 1 which we denoted by ω has a minimal polynomial over $\mathbb{Q}$ of degree 2: it is the cyclotomic polynomial

$$\Phi_3 = \frac{X^3 - 1}{X - 1} = X^2 + X + 1. \tag{6.3}$$

Since $\omega \notin F$, this remains irreducible over F, and $[L : F] = 2$, $[L : \mathbb{Q}] = 6$.

Write $F' = \mathbb{Q}(\omega\alpha)$ and $F'' = \mathbb{Q}(\omega^2\alpha)$. Write $K = \mathbb{Q}(\omega)$. The three cubic fields F, F' and F'' are distinct (prove!) and K is quadratic. We shall show that together with L itself and $\mathbb{Q}$, these are all the intermediate fields.

It is now time to compute $G = Gal(L/K)$. We know that this should be a group of order 6. There are two groups of order 6: a cyclic one, Z_6, and a non-abelian one, S_3. If you did the exercise at the end of the last section, you should not expect Z_6, because we know that L has intermediate fields (namely F, F' and F'') which are not normal over $\mathbb{Q}$. So we should discover S_3. There is a quick way to get it: every $\sigma \in G$ induces a permutation of the 3 roots of $X^3 - 2$, and is determined by this permutation, since the three roots generate L. So we get an *injective* homomorphism from G to S_3. Comparing group orders, this is an isomorphism.

We can also find the structure of G via generators and relations. Let ρ be complex conjugation. Since $\rho(\omega) = \bar{\omega} = \omega^2$ and $\rho(\alpha) = \alpha$, the fixed field of ρ contains F. Since ρ is of order 2, the degree of L over its fixed field must be 2, so the fixed field is just F and

$$Gal(L/F) = \{e, \rho\}. \tag{6.4}$$

Note that ρ exchanges $\omega^2\alpha$ with $\omega\alpha$. Next, consider $Gal(L/K)$, which is of order $3 = [L : K]$. The minimal polynomial of α over K is still $X^3 - 2$, and it splits in L, so there exists a $\sigma \in Gal(L/K)$ mapping α to $\omega\alpha$. Now

$$\sigma(\omega\alpha) = \sigma(\omega)\sigma(\alpha) = \omega \cdot \omega\alpha = \omega^2\alpha \tag{6.5}$$

and likewise $\sigma(\omega^2\alpha) = \alpha$. Thus σ induces a cyclic permutation of order 3 of the roots of $X^3 - 2$. To find the relations that hold between σ and ρ we compute the effect of $\rho\sigma\rho^{-1}$ on α and on ω

$$\begin{aligned} \rho\sigma\rho^{-1}(\alpha) &= \rho\sigma(\alpha) = \rho(\omega\alpha) = \rho(\omega)\rho(\alpha) = \omega^2\alpha \\ \rho\sigma\rho^{-1}(\omega) &= \rho\sigma(\omega^2) = \rho(\omega^2) = \omega. \end{aligned} \tag{6.6}$$

It follows that $\rho\sigma\rho^{-1} = \sigma^2$.

The fields F, F' and F'' are the fixed fields of $\{1, \rho\}, \{1, \rho\sigma\}$ and $\left\{1, \rho\sigma^2\right\}$ respectively, and K is the fixed field of $\left\{1, \sigma, \sigma^2\right\}$. Since these are the only subgroups of G, besides G itself and $\{e\}$, we have found all the subfields of L.

6.2. **A second example.** Let p be a prime number, $\zeta = \exp(2\pi i/p)$ and $L = \mathbb{Q}(\zeta)$. We have seen before that $[L : \mathbb{Q}] = p - 1$ and that $G = Gal(L/\mathbb{Q})$ consists of the $p - 1$ elements σ_a, where $\sigma_a(\zeta) = \zeta^a$ $(1 \le a \le p - 1)$. To see the *group structure* let us compute the effect of $\sigma_a\sigma_b$ on ζ:

$$\sigma_a\sigma_b(\zeta) = \sigma_a(\zeta^b) = (\sigma_a(\zeta))^b = (\zeta^a)^b = \zeta^{ab} = \sigma_{ab}(\zeta). \tag{6.7}$$

Thus the map which assigns to σ_a the element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an isomorphism. We shall now show that $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ is a *cyclic* group.

Lemma 6.1. *Let F be a field, and W a finite subgroup of $F^\times$. Then W is cyclic.*

Proof. We know that W is the product of its p-Sylow subgroups W_p for the p dividing $|W|$. It is enough to show that each W_p is cyclic because the product of cyclic groups of relatively prime orders is again cyclic. Suppose that W_p has p^e elements. If it does not have an element of exact order p^e then all its elements satisfy $x^{p^{e-1}} = 1$, because their order must divide the order of W_p. However, W_p is a subgroup of $F^\times$ and in a *field* a polynomial equation of degree p^{e-1} can have at most p^{e-1} solutions. This shows that W_p must have an element of order p^e so must be cyclic. ∎

We apply this to the field $\mathbb{Z}/p\mathbb{Z}$ and conclude that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group. In particular, for every n dividing $p-1$ there is a unique subgroup H of G, $[G : H] = n$. It follows that there exists a unique field $M \subset L$ such that $[M : \mathbb{Q}] = n$ for each n dividing $p-1$, and these are all the subfields. They are all normal, and their Galois groups are abelian.

Exercise 6.1. *Prove that the unique subfield of degree $(p-1)/2$ is $\mathbb{Q}(\cos(2\pi/p))$.*

Exercise 6.2. *Find all the subfields when $p = 5$ and when $p = 7$. Find generators for these fields over $\mathbb{Q}$.*

It can be proven that the unique quadratic field of L is $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \bmod 4$ and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \bmod 4$.

6.3. **The Galois group of a polynomial.** Galois was not talking about Galois groups of field extensions. Instead he was talking about the (Galois) group of a polynomial. Let $f \in K[X]$ be a polynomial, and L a splitting field of f over K. Then $Gal(L/K)$ is called the Galois group of the polynomial f. Let α_i $(1 \le i \le n)$ be the roots of f. Then any $\sigma \in Gal(L/K)$ permutes the α_i since $\sigma f = f$. Let $\pi(\sigma)$ be the permutation of the roots of the polynomial f induced by σ. Clearly $\pi(\sigma\tau) = \pi(\sigma)\pi(\tau)$ so π is a group homomorphism of $Gal(L/K)$ into S_n. It is injective: if $\pi(\sigma) = 1$ then $\sigma(\alpha_i) = \alpha_i$ for all i, and since $L = K(\alpha_1, \ldots, \alpha_n)$, σ is the identity. We therefore have

$$Gal(L/K) \subset S_n. \tag{6.8}$$

If f is reducible, say $f = gh$ in $K[X]$ then $\sigma g = g$ and $\sigma h = h$, so the roots of g and the roots of h are permuted among themselves. But even if f is *irreducible*, there is no reason to assume that every permutation is allowed. In the two examples above, in the first one we got all of S_3, but in the second we got a cyclic group of order $p-1$, which is far from the full S_{p-1} whose order would be $(p-1)!$.

Exercise 6.3. *Let f be separable and irreducible, so that $n = \deg f$. Prove that $Gal(L/K) = S_n$ if and only if when we adjoin the α_i one-by-one, the minimal polynomial of α_i over $L_{i-1} = K(\alpha_1, \ldots, \alpha_{i-1})$ is of degree $n + 1 - i$.*

6.4. **Algebraic closure.** We have seen that for any polynomial f there is an algebraic extension of K in which f splits. A field $\bar{K}$ containing K is called an *algebraic closure* of K if (a) it is algebraic over K (b) it is algebraically closed: every polynomial over $\bar{K}$ has a root there (hence splits).

Algebraic closures tend to be infinite extensions of the ground field (unless the ground field was already algebraically closed, or close to it, like $\mathbb{R}$). They can be constructed using Zorn's lemma (or the principle of well-ordering) as follows.

Consider the family of all algebraic extensions of K. Define a partial ordering: $L < M$ if there exists a field embedding $L \to M$ which is the identity on K. Notice that such an embedding is in general not unique, and we can not simply order the fields by inclusion because they are not part of a common big set.

If we have a chain L_i in this ordering we can take its union (w.r.t. the chosen embeddings) to get a field which is still algebraic over K (because every element is in one of the L_i hence is algebraic over K), and into which all the L_i embed. We may thus apply Zorn's lemma to deduce that there is a maximal element in the set. This maximal element is algebraic over K. It must also be algebraically closed: otherwise let f be an irreducible polynomial over it of degree > 1. The splitting field of f will be a strictly larger extension, still algebraic over K (remember: an algebraic extension of an algebraic extension is algebraic). By maximality this is impossible. Thus we have constructed an algebraic closure.

It can be shown with not too much trouble that *any two algebraic closures of K are isomorphic over K*. We shall not do it here.

7. Solvability by Radicals

In this section you will need to recall theorems that were proved in the first semester. In particular, it's good to recall what was done on cyclic, abelian and solvable groups, and the proof that the group A_n is simple, so in particular not solvable, for $n$at least 5. You should also review what you have learned about prenutation groups.

7.1. **Historical introduction.** Perhaps the most famous application of Galois theory is to showing that polynomial equations of degree 5 and higher need not be solvable by radicals. Sometimes this is referred to by laymen as the equation "having no solutions". This is nonsense: we have shown once and again in this course that every polynomial equation over a field K has a solution in a suitable extension. We have also shown that $\mathbb{C}$ is algebraically closed, so every equation over $\mathbb{Q}$ has a solution in $\mathbb{C}$.

What we mean by *not being solvable by radicals* is that there is no way to express the solution starting with the coefficients of the polynomial, and using iteratively the four field operations plus the operation of extracting roots (of any order). In fact, $\sqrt{3}$ is just a notation for a root of $X^2 - 3$ that we couldn't express otherwise using the four basic operations, i.e. as a rational number. Similar remark holds for third, fourth and higher roots. There is no reason not to invent a special notation, say

$$\spadesuit(a, b, c, d, e, f) \tag{7.1}$$

for a root of $aX^5 + bX^4 + cX^3 + dX^2 + eX + f = 0$, but you will end up needing infinitely many symbols, and soon you will discover that it is not more economical to invent new notation than to simply say "let α be a root of...". What the theorem we are going to prove says is that it is impossible to reach every algebraic number over $\mathbb{Q}$, if we only adjoin roots of polynomials of the shape $X^n - a = 0$, not even if we iterate the procedure and allow for a numbers from the fields that we got in the previous step of the iteration.

The famous formula for the quadratic polynomial was essentially gotten by the Arabs. The discovery of the formula for a cubic by Tartaglia and Cardano, the secrecy around it and the rivalry between the two, as well as Ferrari's reduction of the quartic to the cubic, make an interesting piece of Renaissance history. You can read about it in the historical introduction to Stewart's book, or in Bell's Men of Mathematics.

We should also be careful about what coefficients we allow from our ground field. For example, if we start from $\mathbb{C}$, then since it is algebraically closed, we don't need even radicals: all roots are already in the ground field. If we start from $\mathbb{R}$, every equation *is* solvable over $\mathbb{R}$ by radicals: in fact square roots suffice. Over finite fields too every equation is solvable by radicals: if α is a root of some $f \in K[X]$ (in an extension of K) and K is finite, then $K(\alpha)$ is a finite field as well. Since the multiplicative group of $K(\alpha)$ has a finite order, every element, in particular α, satisfies $\alpha^N = 1$ for some N (which may be larger than the original degree of f). Thus α is an Nth root of 1.

We shall prove two theorems. The first will show that over $\mathbb{Q}$ there are equations that are not solvable by radicals. Thus $\mathbb{Q}$ is a much more complicated field than the examples given above, of $\mathbb{C}$, $\mathbb{R}$ and the finite fields, at least when it comes to studying its algebraic extensions. The truth is that $\mathbb{Q}$ is extremely complicated: much of the subject of number theory can be regarded as studying finite extensions of $\mathbb{Q}$.

The second theorem will say *that over any field F the general equation of degree ≥ 5 is not solvable by radicals.* What we mean is that we look at the field

$$K = F(s_1, \ldots, s_n) \tag{7.2}$$

where the s_i are independent variables (K is the field of rational functions in n variables over F) and consider the equation

$$f = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n = 0 \tag{7.3}$$

(the alternating signs are just a convention, that will become clear later). Let α be a root of this equation in an extension $K(\alpha)$ of K. In fact we shall show that f is irreducible in $K[X]$, so $K(\alpha) \simeq K[X]/(f)$. Then if $n \geq 5$ one can not express α starting with the elements of K (i.e. the scalars of F and the symbols s_i) using the field operations and radicals. If you think about it a little, it just means that there is no "general formula" for a solution, like the formula

$$\alpha = \frac{s_1 \pm \sqrt{s_1^2 - 4s_2}}{2} \tag{7.4}$$

in the quadratic case.

7.2. **Kummer extensions.** We shall make the assumption

$$char.(K) = 0. \tag{7.5}$$

This is not necessary, but simplifies the presentation (extracting pth roots in a field of characteristic p is a tricky business). Note that all our extensions are therefore separable, so normal = Galois from now on.

Before we discuss solvability by radicals we need to become familiar with the splitting field L of the polynomial $X^n - a$ ($a \in K$). Since

$$(X^n - a, nX^{n-1}) = 1 \tag{7.6}$$

the polynomial $X^n - a$ is separable (here we use the characteristic 0 assumption!). Let $\alpha \in L$ be any root. Then the n roots of $X^n - a$ in L can be written $\alpha_i = \zeta_i \alpha$ ($0 \leq i \leq n-1$) where $\zeta_i^n = 1$, and where we may assume that $\alpha_0 = \alpha$, i.e. $\zeta_0 = 1$. Since the α_i are distinct, the ζ_i are distinct, and there are n of them, so they are *all* the solutions of

$$X^n - 1 = 0. \tag{7.7}$$

This polynomial splits in L as

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta_i). \tag{7.8}$$

The ζ_i form a *subgroup* W_n of $L^\times$ called the *group of roots of unity of order n* (proof: if $x^n = y^n = 1$ then $(xy)^n = 1$ and $(x^{-1})^n = 1$). We have proven in Lemma

6.1 that a finite subgroup of $L^\times$ must be cyclic. Thus W_n is a cyclic group of order n, and if we let ζ be a generator we may reorder the α_i so that

$$\zeta_i = \zeta^i,\ \alpha_i = \zeta^i\alpha. \tag{7.9}$$

Exercise 7.1. *A generator of W_n is called a* primitive *nth root of unity. How many generators does W_n have?*

We now see that L is generated over K by α and ζ, and we look at the tower

$$K \subset M = K(\zeta) \subset L = K(\zeta, \alpha). \tag{7.10}$$

Theorem 7.1. *(i) M/K is an abelian extension (i.e. Galois, with an abelian Galois group) and $Gal(M/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Its order therefore divides $\varphi(n)$ where φ is the Euler phi-function, counting how many residues prime to n there are modulo n.*

(ii) L/M is a cyclic extension (Galois, with a cyclic Galois group) of order dividing n.

(iii) L/K is Galois. If $G = Gal(L/K)$ and $H = Gal(L/M)$ then $H \lhd G$ and both H and G/H are abelian. The group G is therefore (2-step) solvable.

Proof. (i) The extension M/K is the splitting field of $X^n - 1$, so is Galois. If $\sigma \in Gal(M/K)$ then $\sigma(\zeta)$ is in W_n so we let $\chi(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ be the unique integer modulo n for which

$$\sigma(\zeta) = \zeta^{\chi(n)}. \tag{7.11}$$

We now compute

$$\sigma\tau(\zeta) = \sigma(\zeta^{\chi(\tau)}) = \sigma(\zeta)^{\chi(\tau)} = \zeta^{\chi(\sigma)\chi(\tau)} \tag{7.12}$$

so $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$. Applying this to $\tau = \sigma^{-1}$ we see that $1 = \chi(\sigma)\chi(\sigma^{-1})$ so $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$. It follows that

$$\chi : Gal(M/K) \to (\mathbb{Z}/n\mathbb{Z})^\times \tag{7.13}$$

is a group homomorphism. It is injective because $\chi(\sigma) = 1$ means $\sigma(\zeta) = \zeta$, so σ is the identity on M. It follows that $Gal(M/K)$ is isomorphic to its image under χ, which is an abelian subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since the order of a subgroup divides the order of the group

$$[M : K] | \varphi(n). \tag{7.14}$$

(ii) Let $H = Gal(L/M)$. Note that every $\tau \in H$ fixes $\zeta \in M$. Write

$$\tau(\alpha) = \zeta^{\lambda(\tau)}\alpha \tag{7.15}$$

where $\lambda(\tau) \in \mathbb{Z}/n\mathbb{Z}$. We compute

$$\sigma\tau(\alpha) = \sigma(\zeta^{\lambda(\tau)}\alpha) = \zeta^{\lambda(\tau)}\sigma(\alpha) = \zeta^{\lambda(\tau)}\zeta^{\lambda(\sigma)}\alpha = \zeta^{\lambda(\tau)+\lambda(\sigma)}\alpha. \tag{7.16}$$

It follows that

$$\lambda(\sigma\tau) = \lambda(\sigma) + \lambda(\tau) \tag{7.17}$$

so that λ is a homomorphism from H to the additive group $\mathbb{Z}/n\mathbb{Z}$. As before, λ is injective: if $\lambda(\sigma) = 0$, then $\sigma(\alpha) = \alpha$, so σ is the identity on $L = M(\alpha)$. We conclude that H is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, so is cyclic of order dividing n.

(iii) L/K is a Galois extension because it is a splitting field of a separable polynomial. The subfield M is normal over K because it is the splitting field of X^n-1. It follows that $H = Gal(L/M) \lhd G$. Finally H and $G/H = Gal(M/K)$ were computed in (ii) and (i) respectively. ∎

The extension L/M, namely the splitting field of $X^n - a$ over a field containing the nth roots of unity, is called a Kummer extension.

Exercise 7.2. *Can we have $L = M$? When? If $[L : M] = m$, what is the minimal power of a which is an nth power in M?*

7.3. **Radical extensions.** An extension L of K is called *radical* if $L = K(\alpha_1, \ldots, \alpha_r)$ and for every i there exists some N such that

$$\alpha_i^N \in K(\alpha_1, \ldots . \alpha_{i-1}). \tag{7.18}$$

We call the α_i a *radical sequence* for L. For example $\sqrt{\frac{1+2^{1/3}}{1-7^{1/5}}}$ belongs to the radical extension $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ of the rationals where

$$\begin{aligned} \alpha_1^3 &= 2 \in \mathbb{Q} \\ \alpha_2^5 &= 7 \in \mathbb{Q}(\alpha_1) \\ \alpha_3^2 &= \frac{1+\alpha_1}{1-\alpha_2} \in \mathbb{Q}(\alpha_1, \alpha_2). \end{aligned}$$

We say that a polynomial $f \in K[X]$ is *solvable by radicals* if there exists a radical extension L of K in which f splits. Thus all the roots of f, not just one, should be expressible by radicals. Note that the α_i used to exhibit L as a radical extension need not be the roots of f. Note also that we do not insist that the splitting field of f is a radical extension, only that it is contained in one.

Recall that a finite group G is called *solvable* if there exists a chain of subgroups

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_r = \{e\} \tag{7.19}$$

each normal in the previous one, with H_{i-1}/H_i abelian. Call a Galois extension *solvable* if its Galois group is a solvable group.

Theorem 7.2. *If f is solvable by radicals over K, then the Galois group of f is a solvable group.*

Lemma 7.3. *If f is solvable by radicals then its splitting field is contained in a radical extension which is Galois over K.*

Proof. Let L be a radical extension in which f splits. Write $L = K(\alpha_1, \ldots, \alpha_r)$ where the α_i are a radical sequence as above (each a certain root of a number from $K(\alpha_1, \ldots, \alpha_{i-1})$). Let m_i be the minimal polynomial of α_i over K and m the product of the m_i. Let M be a splitting field of m over K. Then M/K is Galois. We shall show that M is still a radical extension of K, so it will be the desired field.

Let $\sigma \in Gal(M/K)$ and $\beta_i = \sigma\alpha_i$. The field

$$\sigma L = K(\beta_1, \ldots, \beta_r) \tag{7.20}$$

is isomorphic to L (via σ) so is also a radical extension of K, and the β_i form a radical sequence. Now for every i and every root β_i of m_i there is an isomorphism of $K(\alpha_i)$ onto $K(\beta_i)$ taking α_i to β_i. This isomorphism can be extended to an automorphism σ of M (note: we may not be able to specify simultaneously $\sigma\alpha_i$ for

two different i's - we work with one index i at a time). It follows that among the collection

$$\{\sigma\alpha_i | 1 \leq i \leq r, \sigma \in Gal(M/K)\} \tag{7.21}$$

we find all the roots of m, so this collection generates M over K. But this collection is clearly a radical sequence, as each 'segment' of it $\sigma\alpha_1, \ldots, \sigma\alpha_r$ is a radical sequence. This shows that M is a radical extension of K as well. ∎

Proof. (of the theorem) We shall use the following group theoretical result: If $G \rhd H$ then G is solvable if and only if both H and G/H are solvable. What this means is that if

$$K \subset M \subset L \tag{7.22}$$

is a tower of finite Galois extensions (all three: L/M, M/K and L/K should be Galois), then L/K is solvable if and only if L/M and M/K are.

Step 1. Assume that f is solvable by radicals, and Σ is its splitting field. We have to show that $Gal(\Sigma/K)$ is solvable. Let, as in the lemma, L be a radical extension containing Σ, which is Galois over K. Applying the remark we just made to $K \subset \Sigma \subset L$ it is enough to show that L/K is solvable. This step allows us to forget f and prove: *a radical Galois extension is solvable.*

Step 2. Let $L = K(\alpha_1, \ldots, \alpha_r)$ where α_i is a radical sequence for L. Let N_i be an integer such that

$$\alpha_i^{N_i} \in K(\alpha_1, \ldots, \alpha_{i-1}). \tag{7.23}$$

Let N be an integer divisible by all the N_i and ζ an Nth root of 1. The group W_N that ζ generates contains all roots of unity of order N_i for all i. Clearly $L(\zeta)/K(\zeta)$ is radical and Galois (a radical sequence for L/K is a radical sequence for it as well). Suppose we have shown that it is solvable. Then, since $K(\zeta)/K$ is abelian and $L(\zeta)/K$ is Galois, $L(\zeta)/K$ is also solvable. A second use of the same remark from the beginning shows now that L/K is solvable. Thus we may assume *without loss of generality* that for each i, $W_{N_i} \subset K$.

Step 3. Let $L_i = K(\alpha_1, \ldots, \alpha_i)$ and $H_i = Gal(L/L_i)$ (write also $H_0 = G$). We shall show that

$$H_{i-1} \rhd H_i \tag{7.24}$$

and that H_{i-1}/H_i is abelian. Here we note that

$$L_i = L_{i-1}(\alpha_i) \tag{7.25}$$

and $\alpha_i^{N_i} \in L_{i-1}$. We assumed that $W_{N_i} \subset K$, so by what we have shown in the theorem on Kummer extensions, L_i/L_{i-1} is Galois with cyclic Galois group. It follows that H_i is normal in H_{i-1} and the quotient is cyclic, hence clearly abelian. ∎

Remark 7.1. *The converse of the Theorem is also true: If L/K is a solvable Galois extension, then L can be embedded in a radical Galois extension of K. We sketch the proof. First, we adjoin to K all roots of unity of order $[L : K]$. To ease the notation, assume that K contained them from the start. Next, there is a tower of fields*

$$K = L_0 \subset L_1 \subset \cdots \subset L_r = L \tag{7.26}$$

such that each layer L_i/L_{i-1} is Galois and abelian (note the L_i need not be Galois over K). Since every finite abelian group is a product of cyclic groups, we may

refine the tower and assume that the layers are cyclic. Note that all roots of unity of order $[L_i : L_{i-1}]$ *are already in* K*. What we need is the following theorem, which we state without proof. It is a* converse *to part (ii) of Theorem 7.1.*

Theorem 7.4. *(Kummer) Let* K *be a field of characteristic 0, and* L/K *a cyclic extension of degree* n*. Assume that* K *contains* W_n*, the group of* n*th roots of unity. Then there exists an* $a \in K$ *such that* $L = K(\alpha)$ *and* $\alpha^n = a$*.*

The theorem remains valid if $char.K$ is relatively prime to $[L : K]$. Cyclic p-extensions in characteristic p have also been studied, by Artin and Schreier.

7.4. **A non-solvable polynomial.** According to the theorem proved above, to give an example of a polynomial which is not solvable by radicals, it is enough to give an example of a polynomial whose splitting field has a non-solvable Gaois group. As we have seen, this can not be done over arbitrary K. We do it with $K = \mathbb{Q}$. First we quote facts from group theory

Theorem 7.5. *The group* A_n *(*$n \geq 5$*) is simple (i.e. has no normal subgroups at all). The group* S_n *(*$n \geq 5$*) is non-solvable.*

Exercise 7.3. *Analyze* S_n *for* $n \leq 4$ *and show that it* is *solvable.*

Lemma 7.6. *Let* G *be a subgroup of* S_p *where* p *is prime that contains a transposition and a cycle of order* p*. Then* $G = S_p$*.*

Proof. Lable the letters so that the transposition is $\tau = (12)$ and the cycle $\sigma = (1a_2a_3...a_p)$. If $a_k = 2$ then replacing σ by σ^{k-1} (which is again of order p since p was prime) we may assume that $a_2 = 2$. We may then rename the remaining letters so that $\sigma = (12...p)$. The group G contains then

$$\sigma^{i-1}\tau\sigma^{1-i} = (i, i+1) \tag{7.27}$$

hence also

$$(1, i+1) = (1, i)(i, i+1)(1, i) \tag{7.28}$$

by induction on i and

$$(i, j) = (1, i)(1, j)(1, i) \tag{7.29}$$

for any i and j. Since every permutation is a product of transpositions, G contains everything. ∎

Lemma 7.7. *Let* $f \in \mathbb{Q}[X]$ *be an irreducible polynomial of prime degree* p *and assume that in* $\mathbb{C}$ f *has two complex roots and* $p - 2$ *real ones. Then the Galois group of* f *is* S_p*.*

Proof. Let L be the splitting field of f and $G = Gal(L/\mathbb{Q})$. We know that $G \subset S_p$ via its action on the p roots. If α is a root of f, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, so

$$p|[L : \mathbb{Q}] = |G|. \tag{7.30}$$

If p divides the order of G, G must contain an element of order p. The only elements of order p in S_p are cycles of order p, so G contains a cycle of order p.

Let ρ be complex conjugation (acting on $\mathbb{C}$). Since L is normal it preserves L, and by assumption it fixes $p - 2$ of the roots, and exchanges the two complex one (which must therefore be complex conjugates of of one another). Thus $\rho \in G$ is a transposition. By the lemma, $G = S_p$. ∎

Corollary 7.8. *If $p \geq 5$ and f is as in the lemma, the Galois group of f is S_p, hence is non-solvable, and f is not solvable by radicals.*

Example 7.1. *Take*

$$f = X^5 - 6X + 3. \tag{7.31}$$

By Eisenstein's criretion (for 3) it is irreducible. Since $f' = 5X^4 - 6$ has two real roots, say $\pm\theta$, and $f(-\theta) > 0 > f(\theta)$, it is easily seen that f has precisely three real roots, in the intervals $(-\infty, -\theta)$ (where $f' > 0$), $(-\theta, \theta)$ (where $f' < 0$) and (θ, ∞) (where $f' > 0$). This polynomial satisfies the conditions of the lemma.

8. The general polynomial equation

8.1. **Transcendental degree.** As we saw before, there exist fields over which *every* polynomial equation is solvable by radicals: algebraically closed fields, $\mathbb{R}$, finite fields... Even over $\mathbb{Q}$, a *specific* polynomial equation of a high degree may well be solvable by radicals: start with any algebraic number α expressed by radicals. It's minimal polynomial $f_\alpha \in \mathbb{Q}[X]$ may well be of a very high degree (from the algorithmic point of view, it is not an easy task to determine f_α!). Now α is contained in a radical extension of $\mathbb{Q}$. The proof of Lemma 7.3 shows that α is in fact contained in a *normal* radical extension of $\mathbb{Q}$. It follows that all the roots of f_α (the *conjugates* of α over $\mathbb{Q}$) are expressible by radicals, so f_α is solvable by radicals.

So what does it mean that *in general* a polynomial of degree ≥ 5 is not solvable by radicals? It means that if we treat the coefficients as "independent parameters", there is no formula expressing the roots in terms of the coefficients, and which uses only radicals, besides the basic four operations.

To make this rigorous we have to talk about transcendental extensions - extensions generated by algebraically independent elements.

Recall that an extension L/K is finitely generated if there are $\alpha_1, \ldots, \alpha_m$ in L such that

$$L = K(\alpha_1, \ldots \alpha_m). \tag{8.1}$$

We do not insist that the α_i are algebraic over K.

A monomial M in the variables $t_1, \ldots, t_n$ is an expression of the forms

$$M = t_1^{e_1} t_2^{e_2} \ldots t_n^{e_n} \tag{8.2}$$

where the $e_i \geq 0$. For example, $t_1^2 t_2 t_3^5$, t_2^2, and $t_1 t_3$ are examples of monomial in three variables. The e_i is called the degree of the monomials in the variable t_i and $\sum e_i$ is called the *total degree* of the monomial, denoted $\deg(M)$. Monomials may be multiplied, and of course $\deg(M_1 M_2) = \deg(M_1) + \deg(M_2)$.

A formal sum

$$P = \sum a_{e_1 e_2 \ldots e_n} t_1^{e_1} t_2^{e_2} \ldots t_n^{e_n} \tag{8.3}$$

involving only finitely many monomials is called a *polynomial* in n variables. The maximum of the degrees of the monomials is called the degree of the polynomial. For example

$$t_1^2 t_2 t_3^5 + 3t_2^2 - 2t_1 t_3 \tag{8.4}$$

is a poynomial of degree 8 in three variables.

The polynomials in $t_1, \ldots, t_n$ with coefficients from K make up a commutative ring denoted

$$K[t_1, \ldots, t_n]. \tag{8.5}$$

This ring is an integral domain: the product of two non-zero polynomials is non-zero. To prove it, notice that for any integral domain R the ring of polynomials in one variable $R[t]$ over R is an integral domain. But

$$K[t_1, \ldots, t_n] = K[t_1, \ldots, t_{n-1}][t_n], \tag{8.6}$$

so the claim is proved by induction on n. It is interesting to note, in passing, that $K[t_1, \ldots, t_n]$ is not a prinicpal ideal domain if $n > 1$ (prove that the ideal $(t_1, \ldots, t_n)$ is not principal). However, it is still a unique factorization domain (the proof of this fact requires some work).

The field of fractions of $K[t_1, \ldots, t_n]$ is denoted by $K(t_1, \ldots, t_n)$ and is called the field of rational functions in n variables.

If L is generated by n elements $\alpha_1, \ldots, \alpha_n$ over K we may define a ring homomorphism

$$\varphi : K[t_1, \ldots, t_n] \to L \tag{8.7}$$

by *substituting* in the polynomial P the value $t_i = \alpha_i$ and *evaluating* it (in L).

The elements α_i are called *algebraically independent* over K if this map is injective: i.e. there is no polynomial relation between the α_i. This is clearly a generalization of the notion of being *transcendental* (when $n = 1$). If this is the case, the map φ extends to an embedding

$$\varphi : K(t_1, \ldots, t_n) \to L. \tag{8.8}$$

Since the image is a subfield of L, but the $\alpha_i = \varphi(t_i)$ generate L, this is onto, so an isomorphism.

Definition 8.1. *Let L be a finitely generated extension of K, and let $\alpha_1, \ldots, \alpha_n$ be any set of generators. If d is the maximal number of α_i which are algebraically independent over K, we call d the* transcendence degree *of L over K,*

$$d = tr.\deg(L/K). \tag{8.9}$$

If $\alpha_1, \ldots, \alpha_d$ are algebraically independent, then they are called a transcendental basis *of L/K. Not that L is then a* finite *(in particular, algebraic) extension of $K(\alpha_1, \ldots, \alpha_d)$ because for each $i \geq d+1$, α_i is algebraic over $K(\alpha_1, \ldots, \alpha_d)$ (otherwise it would form, together with $\alpha_1, \ldots, \alpha_d$, an algebraically independent set of $d+1$ elements).*

Lemma 8.1. *(Steinitz) The transcendence degree is a well defined notion.*

Proof. We have to show that if

$$L = K(\beta_1, \ldots, \beta_m) \tag{8.10}$$

where (after reordering) $\beta_1, \ldots, \beta_e$ are algebraically independent, then $e \leq d$. If $\beta_1, \ldots, \beta_e$ from a maximal algebraically independent subset of β_i, then by the same argument we shall have also $d \leq e$, hence $d = e$.

So suppose $e > d$. Since β_1 is algebraic over $K(\alpha_1, \ldots, \alpha_d)$, there is a polynomial

$$P \in K(\alpha_1, \ldots, \alpha_d)[X] \tag{8.11}$$

annihilating β_1. The coefficients of P are rational functions, so multiplying by a common denominator we may assume they are polynomials in $\alpha_1, \ldots, \alpha_d$. We conclude that there exists a polynomial $P(t_1, \ldots, t_d; X)$ such that $P(\alpha_1, \ldots, \alpha_d; \beta_1) = 0$. The polynomial P must involve one of the t_i, say t_1, otherwise β_1 would be algebraic over K. Thus it can be viewed also as a polynomial equation for α_1 over $K(\beta_1, \alpha_2, \ldots, \alpha_d)$. Looking at the tower

$$K(\beta_1, \alpha_2, \ldots, \alpha_d) \subset K(\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_d) \subset L \tag{8.12}$$

we see that each step is a finite extension: the first, because α_1 is algebraic over $K(\beta_1, \alpha_2, \ldots, \alpha_d)$, and the second because L is already finite over $K(\alpha_1, \alpha_2, \ldots, \alpha_d)$. It follows that $\beta_2 \in L$ is algebraic over $K(\beta_1, \alpha_2, \ldots, \alpha_d)$, so, as before, there exists a polynomial

$$P \in K[t_1, t_2, \ldots, t_d; X] \tag{8.13}$$

such that $P(\beta_1, \alpha_2, \ldots, \alpha_d, \beta_2) = 0$. Now this polynomial must involve one of $t_2, \ldots, t_d$, because had it involved only t_1 and X the set $\{\beta_1, \beta_2\}$ would be algebraically dependent over K, contrary to our assumption. Without loss of generality assume it involve t_2. It can then be viewed as an equation for α_2 over $K(\beta_1, \beta_2, \alpha_3, \ldots, \alpha_d)$. Continuing in this way we can replace every α_i in the first transcendental basis by a β_i. Note that we can keep doing this because we assumed that $e > d$. But at the end we shall reach the conclusion that L is finite hence algebraic over $K(\beta_1, \ldots, \beta_d)$, and if $e > d$ this is a contradiction, because there will have to be some algebraic relation between $\beta_1, \ldots, \beta_{d+1}$.

Note that the proof is very similar in spirit to the familiar proof that the number of elements in a basis of a vector space is independent of the given basis. ∎

Remark 8.1. *One may ask if the dimension $[L : K(\alpha_1, \ldots, \alpha_d)]$ is independent of the chosen transcendental basis. The simplest example shows that this need not be so: let $L = K(t)$, the field of rational functions in one variable. If we take $\alpha = t$ as a transcendental basis, then $[L : K(\alpha)] = 1$. However, $\beta = t^2$ is also a transcendental basis, but $[L : K(\beta)] = 2$ since $X^2 - \beta$ is the minimal polynomial for α over $K(\beta)$.*

Remark 8.2. *A more interesting example is given by*

$$L = \mathbb{C}(X)[Y]/(Y^3 + X^3 - 1). \tag{8.14}$$

It can be shown that the polynomial $Y^3 + X^3 - 1 \in \mathbb{C}(X)[Y]$ is irreducible over $\mathbb{C}(X)$. (Hint: it is enough to show that $1 - X^3$ is not a third power in $\mathbb{C}(X)$.) It follows that if we denote by x and y the classes of X and Y in L, then in the tower

$$\mathbb{C} \subset \mathbb{C}(x) \subset \mathbb{C}(x, y) = L \tag{8.15}$$

the first extension is transcendental, and the second algebraic of degree 3. Thus $\{x\}$ is a transcendental basis and L is of degree 3 over $\mathbb{C}(x)$. The roles of x and y of course could be exchanged: $\{y\}$ is also a transcendental basis, and L is of degree 3 also over $\mathbb{C}(y)$. Is there a transcendental basis $\{z\}$ such that

$$[L : \mathbb{C}(z)] = 1 \text{ or } 2? \tag{8.16}$$

An easy computation shows that if $z = x + y$ then

$$\begin{aligned} 0 &= y^3 + x^3 - 1 = y^3 + (z - y)^3 - 1 \\ &= 3zy^2 - 3z^2y + z^3 - 1 \end{aligned} \tag{8.17}$$

so y satisfies an equation of degree 2 over $\mathbb{C}(z)$, and clearly $L = \mathbb{C}(z, y)$. Thus we can find an element z making the above degree 2. However, we can not find an element z which will make it 1! *This fact requires some algebraic geometry, or at least some ideas that are beyond the scope of our course.*

8.2. **Symmetric polynomials and Newton's theorem.** Let k be a field and

$$L = k(t_1, \dots, t_n) \tag{8.18}$$

the field of rational functions in n variables over k. Let $G = S_n$ act on L by the rule

$$\sigma(f(t_1, \dots, t_n)) = f(t_{\sigma(1)}, \dots, t_{\sigma(n)}). \tag{8.19}$$

It is straightforward to prove that each σ is a field automorphism, and that this is a group action: namely $\sigma(\tau(f)) = (\sigma\tau)(f)$. Moreover, if σ is the trivial automorphism, then it was the trivial permutation to begin with. Thus we found

$$G \subset Aut(L). \tag{8.20}$$

The fixed field $\mathcal{F}(G)$ of G is called the *field of symmetric functions*. The polynomials in it are called the symmetric polynomials.

For example, if $n = 3$ and $f = t_1^2 t_3 + t_2 + t_3^5$ then the permutation $\sigma = (123)$ transforms f to $\sigma f = t_2^2 t_1 + t_3 + t_1^5$ which is a different polynomial. The polynomials $t_1^r + t_2^r + t_3^r$ ($r \in \mathbb{N}$) on the other hand are symmetric.

Consider the polynomial

$$f(X) = (X - t_1)(X - t_2) \dots (X - t_n) \in L[X] \tag{8.21}$$

which is a monic polynomial whose coefficients are themselves polynomials in the t_i. If we extend as usual the action of G from L to $L[X]$, then each $\sigma \in G$ permutes the factors of f, but leaves f itself invariant. Thus the coefficients of f must be symmetric polynomials. They are called the *elementary symmetric polynomials in the t_i*. One usually writes

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n \tag{8.22}$$

so that

$$s_i = \sum_{j_1 < j_2 < \dots < j_i} t_{j_1} \dots t_{j_i} \tag{8.23}$$

is the sum of the $\begin{pmatrix} n \\ i \end{pmatrix}$ possible products of i variables.

Clearly the field $K = k(s_1, \dots, s_n)$ generated by the elementary symmetric polynomials over k is contained in $\mathcal{F}(G)$.

Theorem 8.2. *(i) We have an equality $K = \mathcal{F}(G)$, and $Gal(L/K)$ is $G = S_n$. In particular*

$$[k(t_1, \dots, t_n) : k(s_1, \dots, s_n)] = n!. \tag{8.24}$$

(ii) $\{s_1, \dots, s_n\}$ is a transcendental basis for L over k. In particular, the s_i are algebraically independent ("free variables") over k.

Proof. Consider the tower

$$K = k(s_1, \dots, s_n) \subset \mathcal{F}(G) \subset L = k(t_1, \dots, t_n). \tag{8.25}$$

Galois theory tells us that $L/\mathcal{F}(G)$ is a Galois extension whose group is just $G = S_n$, so in particular

$$[L : \mathcal{F}(G)] = n!. \tag{8.26}$$

On the other hand $f \in K[X]$ because the s_i are its coefficients, and L is its splitting field over K because the t_i are its roots. Since the splitting field of a polynomial of degree n has degree *at most* $n!$ we hae

$$[L : K] \leq n!. \tag{8.27}$$

From here we conclude that $K = \mathcal{F}(G)$ and all the assertions in (i).

To prove (ii) note that the transcendence degree of L over k is n. If d is the maximal number of the s_i which are algebraically independent over k, then the rest of the s_i are algebraic over them. Since the t_i are algebraic over K, L would have then transcendence degree d, so we must have $d = n$. This proves (ii). ∎

The case $n = 2$ of the above should be familiar: take $k = \mathbb{C}$ for example and consider

$$f = X^2 + bX + c \tag{8.28}$$

where $b = -s_1$ and $c = s_2$ are independent parameters. Then $K = \mathbb{C}(b, c)$ is the field of rational functions in the two quantities b and c. The two solutions of $f = 0$ are

$$t_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2} \tag{8.29}$$

and they generate $L = K(\sqrt{\Delta})$ where $\Delta = b^2 - 4c$ is the discriminant. Clearly $[L : K] = 2!$.

Corollary 8.3. *Every symmetric function in the t_i is a rational function in the elementary symmetric polynomials s_i.*

Proof. This is just a restatement of $K = \mathcal{F}(G)$. ∎

Newton proved, long before Galois, and by direct computations, a stronger theorem: every symmetric polynomial is a polynomial in the elementary symmetric polynomials. For example, in two variables

$$t_1^2 + t_2^2 = s_1^2 - 2s_2 \tag{8.30}$$

and in three variables

$$t_1^2 + t_2^2 + t_3^2 = s_1^2 - 2s_2 \tag{8.31}$$

and

$$t_1^3 + t_2^3 + t_3^3 = s_1^3 - 3s_1 s_2 + 3s_3. \tag{8.32}$$

8.3. **Insolubility of the general polynomial of degree ≥ 5.** We can now treat the s_i as independent variables and call

$$f = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n \in K[X] \tag{8.33}$$

the *general polynomial* of degree n. The field L is its splitting field. If $n \geq 5$ then $Gal(L/K)$ is insoluble, so by the Theorem 7.2 f is *not* solvable by radicals over K, namely one can not express the roots t_i in terms of the coefficients s_i using radicals only.

8.4. **Solving cubics and quadrics.**

9. Complements

9.1. **Finite fields.** A finite field is always of finite characteristic p (otherwise it would contain $\mathbb{Q}$). In this section we let F be a finite field and p its characteristic. Then F contains the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of p elements.

Proposition 9.1. *(i) $|F| = p^n$ for some n*

(ii) $F^\times$ is a cyclic group of order $p^n - 1$

(iii) F is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, and consists of the p^n roots of this poynomial, which are all distinct.

(iv) F is a Galois extension of $\mathbb{F}_p$, and $Gal(F/\mathbb{F}_p)$ is a cyclic group, generated by the Frobenius automorphism

$$\varphi(x) = x^p. \tag{9.1}$$

Proof. (i) Let $n = [F : \mathbb{F}_p]$, which is finite, since F is a finite set, so clearly its dimension over $\mathbb{F}_p$ is also finite. If $\omega_1, \ldots, \omega_n$ is a basis of F over $\mathbb{F}_p$ then every element of F has a unique expression as $\sum a_i\omega_i$ with $a_i \in \mathbb{F}_p$. The number of such expressions is p^n.

(ii) The multiplicative group $F^\times$ is of course of order $p^n - 1$. We have proved that for *every* field, a finite subgroup of $F^\times$ is cyclic. In this case $F^\times$ itself is finite, hence is cyclic.

(iii) Every element of $F^\times$ satisfies

$$x^{p^n-1} = 1 \tag{9.2}$$

because in any group the order of each element divides the order of the group. Thus every element of F satisfies $x^{p^n} = x$ (note that 0 too satisfies this equation). The polynomial

$$f = X^{p^n} - X \tag{9.3}$$

has derivative $f' = -1$ (because in F we have $p = 0$), so $(f, f') = 1$ and f is separable. Another way to see it is to note that it already has $p^n = \deg(f)$ distinct roots, namely all the different elements of F. In any case we get that

$$X^{p^n} - X = \prod_{\alpha \in F} (X - \alpha), \tag{9.4}$$

and that F consists of the set of its roots, so is clearly generated by them, proving that it is the splitting field of f.

(iv) F is Galois as the splitting field of a separable polynomial. In any field of characteristic p, the Frobenius φ is an (injective) endomorphism. Since F is finite, it is also surjective, so it is an automorphism. Let m be the order of $\varphi \in Gal(F/\mathbb{F}_p)$. Then m is the first natural number such that

$$\varphi^m(x) = x^{p^m} = x \tag{9.5}$$

for all $x \in F$. But the equation $X^{p^m} - X = 0$ has at most p^m roots, so the first m for which it holds is $m = n$. Thus φ is of order n, and generates a cyclic subgroup of order n in $Gal(F/\mathbb{F}_p)$. Since

$$|Gal(F/\mathbb{F}_p)| = [F : \mathbb{F}_p] = n \tag{9.6}$$

the Galois group is just the cyclic group generated by φ. ∎

Don't confuse the fact that $F^\times$ is cyclic with the fact that $Gal(F/\mathbb{F}_p)$ is cyclic!

Corollary 9.2. *Every two finite fields of the same cardinality are isomorphic.*

Proof. They must be of the same characteristic p. Let their cardinality be p^n. Then both are splitting fields of the same polynomial, by (iii), so they are isomorphic. ∎

In the proposition we *assumed* that a field of cardinality p^n was given, and analyzed its structure and the structure of its Galois group over the prime field. Now we prove existence.

Theorem 9.3. *(i) For every n there* exists *a field of p^n elements, unique up to isomorphism. This field is denoted $\mathbb{F}_{p^n}$ and called the Galois field of p^n elements.*

(ii) The subfields of $\mathbb{F}_{p^n}$ are in one-to-one correspondence with the divisors *$m|n$. In particular*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Leftrightarrow m|n. \tag{9.7}$$

Proof. (i) Let F be the splitting field of $f = X^{p^n} - X$ over $\mathbb{F}_p$. By definition it is the minimal field containing $\mathbb{F}_p$ and all the roots of f. However, the *set* of all the p^n roots is already closed under addition, subtraction, multiplication and inverse, because it is the set of fixed points of φ^n. Thus this set is the field F.

(ii) By Galois theory, and the fact that $Gal(F/\mathbb{F}_p)$ is cyclic, there is a subfield for each subgroup of $Gal(F/\mathbb{F}_p)$. But the subgroups are just those generated by φ^m for $m|n$. Now the fixed field of φ^m is the set of elements satisfying $\varphi^m(x) = x^{p^m} = x$, which is just $\mathbb{F}_{p^m}$. ∎

Corollary 9.4. *The polynomial $X^{p^m} - X$ divides $X^{p^n} - X$ if and only if $m|n$.*

Proof. The polynomial $X^{p^m} - X$ divides $X^{p^n} - X$ if and only if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, so the corollary follows from (ii). ∎

Of course, the corollary must have a direct elementary proof, that does not involve Galois theory. Suppose that $n = md$. Then

$$p^n - 1 = (p^m - 1)(p^{m(d-1)} + p^{m(d-2)} + \cdots + p^m + 1) \tag{9.8}$$

and quite generally if $a = bc$ then $X^b - 1$ divides $X^a - 1$:

$$X^a - 1 = (X^b - 1)(X^{b(c-1)} + \cdots + X^b + 1) \tag{9.9}$$

so $X^{b+1} - X$ divides $X^{a+1} - X$. We leave a direct proof of the converse as an exercise.

Note that $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is of order $d = n/m$ and is generated by φ^m.

A field is called *perfect* if all its finite extensions are separable. Fields of characteristic 0 are perfect. We have now seen that finite fields are also perfect. On the other hand we have seen before that $\mathbb{F}_p(t)$ is not perfect.

9.2. **The theorem on the primitive element.** Many times in the course we have separated the discussion of field extensions first to a *simple* extension, $L = K(\alpha)$, then to a finitely generated extension which we could access via a tower of simple extensions. It turns out that in many cases, *every* finite extension is simple, i.e. generated by one element. For example, the field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. In fact, every finite extension in characteristic 0 is simple. More generally we have the following.

Theorem 9.5. *Let L/K be a finite* separable *extension. Then $L = K(\alpha)$ for some α.*

Proof. If K is finite, then L is also finite, $L^\times$ is a cyclic group, so we can take α to be its generator. It clearly generates L as an extension of K. Assume from now on that K is infinite. Since L is separable, it can be embedded in a normal and separable extension M of K. (Proof: Let α_i be a finite set of generators of L over K, and f_i their minimal polynomials over K, which are separable by assumption. Any two f_i are either equal or relatively prime. Let f be the product of the f_i without repetitions. Then f is again separable, and we may take M to be its splitting field.) Then M/K is Galois, so has only finitely many intermediate fields $K \subset F \subset M$ (because the Galois group $Gal(M/K)$ has only finitely many subgroups). *A fortiori* there are only *finitely many* intermediate fields

$$K \subset F \subset L. \tag{9.10}$$

It is only this fact, together with the infinitude of K, that we are going to use in the proof. We remark that this property (of having only finitely many intermediate fields) holds also in some inseparable extensions, but there are inseparable extensions of finite degree with infinitely many intermediate fields!

Assume that our conclusion is false, and let $K(\alpha)$ be a *maximal* field inside L which is a simple extension of K. Then $K(\alpha)$ is not L, so let $\beta \in L$, $\beta \notin K(\alpha)$. Consider the fields

$$F_t = K(\alpha + t\beta) \tag{9.11}$$

for $t \in K$, which are all simple extensions of K inside L. Since K is infinite but there are only finitely many fields between K and L, two of these fields must be equal:

$$K(\alpha + t_1\beta) = K(\alpha + t_2\beta). \tag{9.12}$$

Call this field F. It contains both $\alpha + t_1\beta$ and $\alpha + t_2\beta$. Solving the linear equations for α and β (recall the $t_i \in K$) we see that F contains both α and β. Thus F is a proper extension of $K(\alpha)$ which is still simple. This contradiction shows that we must have had $L = K(\alpha)$. ∎

9.3. **Regular polygons.** For which n can we construct the regular polygon with n sides from $\{(0,0),(1,0)\}$ using ruler and compass only? Clearly this is the same as constructing the angle $2\pi/n$, or better, the point $Q_n = (\cos(2\pi/n), \sin(2\pi/n))$. Assume first that $n = p$ is an odd prime.

The field $K_p = \mathbb{Q}(\cos(2\pi/p), \sin(2\pi/p))$ is contained in $L_p = K_p(i) = \mathbb{Q}(\zeta_p, i) = \mathbb{Q}(\zeta_{4p})$ where

$$\zeta_n = \exp(2\pi i/n) = \cos(2\pi/n) + i\sin(2\pi/n). \tag{9.13}$$

We have $[L_p : K_p] = 2$ (why?), and $[L_p : \mathbb{Q}] = 2(p-1)$. To compute the last degree recall that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, and that i does not lie in $\mathbb{Q}(\zeta_p)$. If you are unable to prove this fact at this point, do not worry. You may assume that $[L_p : \mathbb{Q}] = 2(p-1)$ *or* $p-1$ and proceed. Thus if $p-1$ is not a power of 2, $[K_p : \mathbb{Q}]$ is not a power of 2, and we *can not* construct Q_p using ruler and compass only (see Corollary 1.2).

If $p-1$ is a power of 2, then $[K_p : \mathbb{Q}]$ is also a power of 2. Moreover, L_p is a Galois extension with abelian Galois group (because it is a cycoltomic extension),

so the same applies to $K_p/\mathbb{Q}$. Every abelian group G of order 2^m has a sequence of subgroups

$$G = H_0 \supset H_1 \supset H_2 \cdots \supset H_m = \{e\} \tag{9.14}$$

with $[G : H_k] = 2^k$. It follows, by Galois theory, that there is a sequence of fields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_m = K_p \tag{9.15}$$

such that $F_k = F_{k-1}(\sqrt{\alpha_k})$ is a quadratic extension.

Lemma 9.6. *(i) If S is a set of points that can be constructed by ruler and compass (beginning with $(0,0)$ and $(1,0)$), then every number from $\mathbb{Q}(S)$ is constructible (we say that the number α is constructible if the point $(\alpha, 0)$ is constructible).*

(ii) If α is constructible, so is $\sqrt{\alpha}$.

Proof. (i) Left as an exercise (it was on one of the HW problems): given α and β, you have to find ways to construct the numbers $\alpha + \beta$, $\alpha - \beta$ (clear), $\alpha\beta$ and α/β (use similar triangles and proportionality).

(ii) Draw a circle with diameter AB of length $1 + \alpha$. On AB mark the point P which is at distance α from A and distance 1 from B. Erect a perpendicular line through P, and let Q be its intersection with the circle. Then $|PQ| = \sqrt{\alpha}$ (elementary geometry). ∎

Corollary 9.7. *All the numbers in K_p are constructible.*

Proof. Using the Lemma inductively, we see that all the numbers from F_k are constructible for $k = 0, 1, \ldots, m$. ∎

Theorem 9.8. *If $n = p$ is an odd prime then the regular polynomial of p sides is constructibe if and only if*

$$p = 2^r + 1$$

for some r.

Proof. We have seen above that if $p - 1$ is not a power of 2, then the point Q_p is not constructible. If $p - 1$ *is* a power of 2, then the coordinates of Q_p lie in K_p, so by the last corollary are constructible. ∎

More generally, one can show the following.

Theorem 9.9. *The regular polygon of n sides can be constructed by ruler and compass if and only if*

$$n = 2^e p_1 p_2 \ldots p_g \tag{9.16}$$

where p_i are distinct odd primes of the form $2^{r_i} + 1$.

Primes of the form $2^r + 1$ are called Fermat primes. It is easy to show that if $p = 2^r + 1$ is a prime then r itself must be a power of 2, so

$$p = 2^{2^s} + 1. \tag{9.17}$$

Indeed, if $r = dt$ with d an *odd*= od^2 divisor then

$$2^r + 1 = (2^t + 1)(2^{(d-1)t} - 2^{(d-2)t} + 2^{(d-3)t} - \cdots + 1). \tag{9.18}$$

It is unknown whether there are infinitely many Fermat primes. The largest one known is

$$65537 = 2^{2^4} + 1. \tag{9.19}$$

10. Review Problems

1) For any finite group G show that there is a field K, and a finite Galois extension L/K with $Gal(L/K) \simeq G$. (Hint: we did in class the case $G = S_n$).

2) Let M/K be a finite field extension, and let L and F be two intermediate fields such that L/K and F/K are both Galois. Assume that $M = L \cdot F$. Show that M/K is also Galois and that there is an injective homomorphism

$$Gal(M/K) \hookrightarrow Gal(F/K) \times Gal(L/K).$$

Conclude that if both F/K and L/K are abelian extensions, so is M/K.

3) Let L/K be a finite Galois extension and $f \in K[X]$ irreducible. Let

$$f = f_1 \dots f_k \tag{10.1}$$

be the factorization of f into a product of irreducibles in $L[X]$. Prove: (i) the degrees of the f_i are equal, (ii) k divides $[L : K]$ (iii) If $(\deg(f), [L : K]) = 1$ then f remains irreducible over L. (Hint: prove that $Gal(L/K)$ permutes the f_i *transitively*).

4) Let $L = \mathbb{R}(t)$ be the field of rational functions in t over $\mathbb{R}$. Let $\sigma \in Aut(L)$ fix $\mathbb{R}$ and take t to

$$\sigma(t) = \frac{1}{1-t}.$$

Let G be the group generated by σ and let $K = \mathcal{F}(G)$ be its fixed field. Prove that $[L : K] = 3$.

5) Give an example of three fields $L \supset K \supset F$ such that L/K and K/F are finite Galois, but L/F is not Galois. Justify all your claims.

6) Let L be a finite Galois extension of K, $G = Gal(L/K)$, and $\alpha \in L$. Let $H = Gal(L/K(\alpha))$, and let $\sigma_1, \dots, \sigma_r \in G$ be coset representatives for G/H. Prove that the irreducible polynomial of α over K is

$$f(X) = (X - \sigma_1(\alpha)) \cdots (X - \sigma_r(\alpha)).$$

7) Let $\alpha, \beta \in \mathbb{C}$. Prove that if $\alpha + \beta$ and $\alpha\beta$ are both algebraic (over $\mathbb{Q}$), then α and β are algebraic.

8) Prove that the product of all the non-zero elements in a finite field is -1.

9) Prove that the irreducible factors of $X^{p^4} - X$ over $\mathbb{F}_p$ are of degrees $1, 2$ or 4. How many irreducible factors are there of each degree?

10) Prove that $L = \mathbb{Q}(\sqrt{3 + \sqrt{5}})$ is a Galois extension of $\mathbb{Q}$. Find $[L : \mathbb{Q}]$ and describe the structure of $Gal(L/\mathbb{Q})$.

11) What is the minimal polynomial of $\sqrt{3} + \sqrt{-2}$ over $\mathbb{Q}$? Justify all your claims.

12) Determine the Galois group of the splitting field of $X^3 + 2X - 2$ (i) over $\mathbb{Q}$ (ii) over $\mathbb{F}_3$.