FIELD EXTENSIONS

0. Three preliminary remarks. Every non-zero homomorphism between fields is injective; so we talk about *field extensions* $F \subset K$.

Every field F is an extension of $\mathbb{Q}$ (in the case when $1 \in F$ has an infinite additive order), or of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (when 1 has finite, and necessarily prime order, p). We say that the field has *characteristic* $\operatorname{char} F = 0$ and $\operatorname{char} F = p$ respectively.

Given a field extension $K \supset F$, one can consider K as a vector space over F. We write $[K : F] := \dim_F K$ for the dimension of this vector space, finite or infinite. It is called the *degree* of the extension.

1. Algebraic and transcendental elements. Given $K \supset F$, an element $\alpha \in K$ is called *algebraic over* F, if it is a root of a polynomial with coefficients in F, and *transcendental over* F otherwise.

The intersection of all subfields in K containing F and α is obviously a field, which is denoted $F(\alpha)$. It is said to be obtained by "adjoining α to F".

When α is transcendental, the homomorphism $F[x] \to F(\alpha) : x \mapsto \alpha$ is injective (because all $\alpha^k, k = 0, 1, 2, \dots$ are linearly independent over F), and hence $F(\alpha)$ is identified with the field of fractions of $F[x]$, i.e. with the field of rational functions $F(x)$. We have $[F(\alpha) : F] = \infty$.

When α is algebraic, denote by $f = x^n + a_1 x^{n-1} + \dots + a_n$ the monic minimal degree polynomial with coefficients from F, such that $f(\alpha) = 0$. It is called the *minimal polynomial of* α. Clearly, f is irreducible in $F[x]$ (for if $f = gh$, then $g(\alpha) = 0$ or $h(\alpha) = 0$). Therefore the ideal (f) is maximal, and is the kernel of the homomorphism $F[x] \to F(\alpha) : x \mapsto \alpha$. Thus, $F(\alpha) = F[x]/(f)$. In this case the degree $[F(\alpha) : F]$ equals n, the degree of the minimal polynomial f, since $1, \alpha, \dots, \alpha^{n-1}$ form a basis of $F[x]/(f)$ over F.

`Key Lemma.` *Let $f \in F[x]$ be irreducible, and let $K \supset F$ be any field containing F. Then the embeddings $\sigma : F[x]/(f) \hookrightarrow K$ over F (i.e. such that $\sigma|_F = \mathrm{id}_F$) are in one-to-one correspondence with roots $\alpha \in K$ of f in K.*

`Proof.` Indeed, given σ, it maps the class of x to $\alpha \in K$ which satisfies $f(\alpha) = 0$. Conversely, given $\alpha \in K$ satisfying $f(\alpha) = 0$, the ring homomorphism $F[x] \to K$, defined to be identical on constants $F \subset F[x]$ and mapping x to α, factors through the projection $F[x] \to F[x]/(f)$, and thus defines an embedding of the field $F[x]/(f)$ into K. Obviously the embeddings constructed from different roots of f in K are different, e.g. because the images of the class of x are not the same.

`Examples.` (a) $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[x]/(x^2+1)$, and $[\mathbb{C} : \mathbb{R}] = 2$. Replacing i with $-i$ yields another identification of $\mathbb{R}[x](x^2+1)$ with $\mathbb{C}$.

(b) For a prime p, and any $n > 0$, $x^n - p$ is irreducible over $\mathbb{Q}$ (by Eisenstein's criterion), and hence $[\mathbb{Q}\left(\sqrt[n]{p}\right) : \mathbb{Q}] = n$. In fact the polynomial has n roots in $\mathbb{C}$: one real positive, and the others differing from it by a factor $e^{2\pi ik/n}$, $k = 1, \ldots, n-1$. Respectively, $\mathbb{Q}[x]/(x^n - p)$ has n embeddings into $\mathbb{C}$. The *ranges* of different embeddings can coincide or not. E.g., for even n, two of the embeddings are real, i.e. land in $\mathbb{R}$. They correspond to the real roots $\pm\sqrt[n]{p}$, and have the same range, i.e. define the same subfield in $\mathbb{R}$ isomorphic to $\mathbb{Q}[x]/(x^n - p)$. Replacing $+\sqrt[n]{p}$ with $-\sqrt[n]{p}$ results in an *automorphism* of the subfield. Of course, it corresponds to the automorphism of $\mathbb{Q}[x]/(x^n - p)$ induced by $x \mapsto -x$, which for even n is a symmetry of the polynomial $x^n - p$.

2. Algebraic extensions. An extension $K \supset F$ is called *algebraic* if every element of K is algebraic over F. Clearly, a *finite* extension (i.e. an extension of finite degree) is algebraic. Indeed, if $[K : F] = n$, then for any $\alpha \in K$, $1, \alpha, \ldots, \alpha^n$ are linearly dependent over F, i.e. α is a root of a polynomial of degree $\leq n$ with coefficients from F. The converse is false, of course: there are algebraic extensions of infinite degrees.

We will show that in any field extension $L \supset F$, the set

$$\widehat{F} := \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$$

is a subfield, and is the largest algebraic extension of F inside L.

`Proposition.` *Let $F \subset K \subset L$ be a tower of field extensions, $\{\alpha_i\}$ a basis of K over F, and $\{\beta_j\}$ is a basis of L over K (possibly infinite). Then $\{\alpha_i\beta_j\}$ form a basis of L over F.*

`Proof.` Every $c \in L$ is a (finite) linear combination $\sum_j b_j\beta_j$ where $b_j \in K$ (and all but finitely many $= 0$). Each non-zero $b_j = \sum_\alpha a_{ij}\alpha_i$, where $a_{ij} \in F$ (again, all but finitely many $= 0$). Therefore $c = \sum_j \sum_i a_{ij}(\alpha_i\beta_j)$, i.e. L is spanned by $\alpha_i\beta_j$. To show they are linearly independent, take $c = 0$. From $\sum_j(\sum_i a_{ij}\alpha_i)\beta_j = 0$ and linear independence of β_j over K, we conclude that $\sum_i a_{ij}\alpha_i = 0$ for every j. Now from linear independence of α_i over F, we conclude that all $a_{ij} = 0$.

`Corollary 1.` *$[L : F] = [L : K][K : F]$, that is, $[L : F] < \infty$ if and only if both $[L : K], [K : F] < \infty$, and when they are, the degree is multiplicative.*

`Corollary 2.` *If $\alpha, \beta \in K$ are algebraic over $F \subset K$, then $\alpha + \beta, \alpha\beta, \alpha/\beta$ are algebraic over F.*

`Proof.` Indeed, if $[F(\alpha) : F] < \infty$, and $[F(\beta) : F] < \infty$, then $[(F(\alpha))(\beta) : F(\alpha)] \leq [F(\beta) : F] < \infty$, and hence $F(\alpha, \beta) := (F(\alpha))(\beta)$ (which is the smallest extension of F containing both α and β) has finite degree over F. Therefore all elements of it, including $\alpha + \beta$, $\alpha\beta$, α/β are algebraic.

`Corollary 3.` *If $K \supset F$ is algebraic, and $L \supset K$ is algebraic, then $L \supset F$ is algebraic.*

`Proof.` Let $\alpha \in L$ be a root of a polynomial $x^n + a_1 x^{n-1} + \cdots + a_n$ with coefficients from K. Since $a_1, \ldots, a_n \in K$ are algebraic over F, the field $F(a_1, \ldots, a_n, \alpha)$, obtained by consecutively adjoining α_1 to F, a_2 to $F(a_1)$, etc., and finally α to $F(a_1, \ldots, a_n)$, has finite dimension as a vector space over F. Therefore α is algebraic over F.

`Corollary 4.` *The field $\widehat{F}$ of all elements of $K \supset F$ algebraic over F is a subfield, and moreover, all $\alpha \in K - \widehat{F}$ are transcendental not only over F, but also over $\widehat{F}$.*

`Proof.` Corollary 2 shows that $\widehat{F}$ is closed with respect to the field operations, and Corollary 3 implies that all elements of K algebraic over $\widehat{F}$ lie in $\widehat{F}$.

`Example.` Complex numbers algebraic over $\mathbb{Q}$ form the field $\overline{Q} \subset \mathbb{C}$ of *algebraic numbers*. Of course, it has infinite (though countable) degree over $\mathbb{Q}$, e.g. because for any n, $\overline{\mathbb{Q}}$ contains $\mathbb{Q}\left(\sqrt[n]{2}\right)$ of degree n.

3. Straightedge and compass constructions. Here we will show that the divisibility property from Corollary 1 is already a powerful tool for resolving some ancient conundrums of elementary geometry.

A novice to straightedge-and-compass constructions should begin with solving the following exercises:

- Given two segments, construct their sum and their difference.
- At a given point on a line, erect the perpendicular it.
- From a given point outside a line, drop a perpendicular to it.
- Through a given point outside a line, draw a line parallel to it.
- Bisect a given angle.

Practitioners of straightedge-and-compass constructions are familiar with the following trick reducing geometry to algebra. Whenever the length of the desired segment can be computed in terms of given lengths using arithmetic operations and square roots, the desired segment can be constructed by straightedge and compass. Namely, the first step is to take one of the given lengths for the unit of measure (or pick any, if none is given). Next, one invokes

`Thales' theorem:` *Parallel lines cut out on the sides of an angle proportional segments.*

Using it, the products and ratios of given lengths can be constructed (see Figures A,B). Finally, by finding three similar right triangles on Figure C, one can figure out how to construct the square root of a given segment.

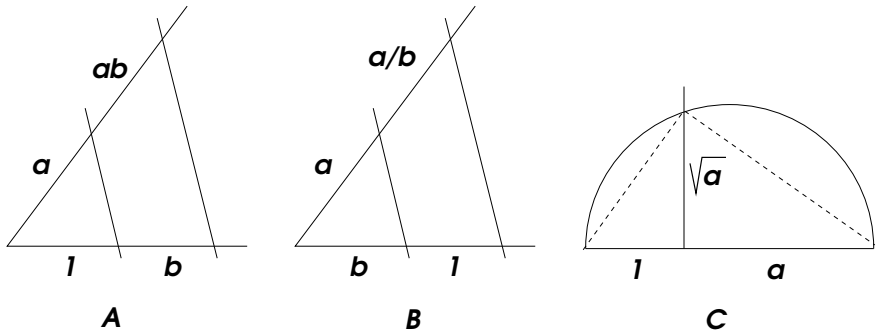

FIGURE 1. Straightedge-and-compass constructions

To translate the problem of possibility of geometric constructions into the language of field extensions, we note that once a unit segment is chosen, one can construct on a number line all points representing rational numbers. In a problem, when some other lengths $d_1, \ldots, d_N$ are given, one can therefore construct all points on the number line representing elements of the field $F := \mathbb{Q}(d_1, \ldots, d_N)$. The previous constructions show that any numbers obtained by a succession of *quadratic* extensions of the field F, (i.e. extensions $F = F_0 \subset F_1 \subset \cdots \subset F_N \subset \mathbb{R}$, where each $F_s = F_{s-1}(\sqrt{a})$), are also constructible. Equivalently, all points on the plane whose coordinates belong to F_N, can be constructed from the given data by straightedge and compass. We claim that the converse is also true.

`Theorem.` *A point on the plain $\mathbb{R}^2 \supset F^2$ is constructible by straightedge and compass if and only if its coordinates belong to a field $E \subset \mathbb{R}$ obtained from F by a finite succession of quadratic extensions.*

`Proof.` The allowed geometric constructions are successions of the following operations:

(i) Drawing a line through previously constructed points.

(ii) Drawing a circle of a previously constructed radius centered at a previously constructed point.

(iii) Constructing a new point by intersecting two previously constructed lines.

(iv) Constructing new points by intersecting a circle and a line, both previously constructed.

(v) Constructing new points by intersecting two previously constructed circles.

In operation (i), the equation of the new line has coefficients in the same field E where the coordinates of the given points $(x_1, y_1), (x_2, y_2)$ belong: $(y_2 - y_1)(x - x_1) = (x_2 - x_1)(y - y_1)$.

In operation (ii), the equation of the new circle has coefficients in the same field E where the coordinates of the circle's center (x_0, y_0) and the radius r lie: $(x - x_0)^2 + (y - y_0)^2 = r^2$, or equivalently: $x^2 + y^2 - 2x_0x - 2y_0y = r^2 - x_0^2 - y_0^2$.

In operation (iii), the intersection point (x_0, y_0) of two lines is found by solving linear equations $a_1x_0 + b_1y_0 = c_1,\ a_2x_0 + b_2y_0 = c_2$, and thus x_0, y_0 lie in the same field E where the coefficients of the equations lie.

The operation (iv) leads to solving a quadratic equation with coefficients in the field E where the coefficients of the equations of the circle and the line lie. Thus, the coordinates of the newly constructed point lie in a quadratic extension $E(\sqrt{d})$, where $d \in E$ is the discriminant of the quadratic equation.

Finally, the operation (v) consists in solving the system of equations

$$x^2+y^2-2x_1x-2y_1y = r_1^2-x_1^2-y_1^2,\ \ x^2+y^2-2x_2x-2y_2y = r_2^2-x_2^2-y_2^2,$$

where $x_i, y_i, r_i \in E$. Note however, that the difference of the two equations is linear, because the purely quadratic terms $x^2 + y^2$ cancel out! This reduces case (v) to case (iv), and thus also results in a quadratic extension $E(\sqrt{d})$ for some $d \in E$.

`Corollary 1.` *Duplicating the cube by straightedge and compass is impossible.*

This is the classical problem of constructing a cube of twice the volume of a given one. To solve it, one needs to construct from the edge 1 of the given cube the edge $\sqrt[3]{2}$ of the "duplicate" cube. For this, a tower of quadratic extensions $\mathbb{Q} \subset F_1 \subset \cdots \subset F_N$ such that $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset F_N$, is needed. But the degree $[F_N : \mathbb{Q}] = 2^N$, while the degree of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ equals 3. Since 3 does not divide 2^N, the required extension does not exist.

Another puzzle that resisted the efforts of best ancient geometers was the problem of trisecting angles. If such a construction existed, it would apply to the angle of 60° to yield a 20° angle. Since the angle of 60° is easily constructible (together with an equilateral triangle), this would make $2\cos 20^\circ$ constructible. We have however $\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta = 4\cos^3\theta - 3\cos\theta$. Since $\cos 60^\circ = 1/2$, we find

a cubic equation for $x = 2\cos 20^\circ$: $x^3 - 3x - 1 = 0$. The polynomial has no rational roots, and hence is irreducible over $\mathbb{Q}$. This shows that $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$, and results in the following

Corollary 2. Trisecting (60° and hence) arbitrary angles by straightedge and compass is impossible.

4. Algebraically closed fields. A field K is called *algebraically closed* if it has no non-trivial algebraic extensions. Equivalently: every polynomial of degree > 1 with coefficients from K is reducible; or equivalently has a root in K; or equivalently factors over K into linear factors. By the Fundamental Theorem of Algebra, $\mathbb{C}$ is algebraically closed. Therefore the field $\overline{\mathbb{Q}}$ of algebraic numbers is algebraically closed: by Corollary 4, complex roots of polynomials with algebraic coefficients lie in $\overline{\mathbb{Q}}$.

`Theorem.` *Every field F has an algebraic extension $\overline{F} \supset F$ which is algebraically closed. Such an extension is unique in the sense that another such extension $\overline{F}' \subset F$ can be identified with $\overline{F}$ by an isomorphism identical on F.*

`Lemma 1.` *Every field F has an algebraically closed extension.*

`Proof` (E. Artin). For every polynomial $f \in F[x]$ of degree > 0 introduce a variable x_f, and consider the ring $F[S]$ where $S = \{x_f\}$. The ideal $I \subset F[S]$ generated by $f(x_f)$ is non-trivial. Indeed, suppose

$$1 = \sum_{i=1}^{n} g_i(x_1, \ldots, x_N) f_i(x_i), \quad x_i := x_{f_i},\ i \le n \le N, \text{ and } g_i \in F[S].$$

Let $K \supset F$ be a finite extension where each f_i has a root, α_i. Then taking $x_i = \alpha_i$ for $i \le n$ and $x_i = 0$ for $i > n$, we arrive at a contradiction: $1 = 0$.

Let $M \supset I$ be a maximal ideal in $F[S]$ (Zorn's lemma!) Then $L_1 := F[S]/M$ is a field in which every polynomial $f \in F[x]$ has a root (the image of x_f in the quotient).

Now, by induction we construct a tower of field extensions

$$F \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \ldots$$

such that every polynomial from $L_n[x]$ of degree > 0 has a root in L_{n+1}.

Let $L := \cup_{n=1}^{\infty} L_n$. It is a field, since any $\alpha, \beta \in L$ lie in some L_n together with $\alpha + \beta$, $\alpha\beta$, and α/β if $\beta \neq 0$. Every polynomial $f \in L[x]$ has coefficients in some L_n and hence a root in L_{n+1}, if $\deg f > 0$.

Thus, L is algebraically closed: every polynomial $f \in L[x]$ of degree > 0 has a root $\alpha \in L$, and hence $f(x) = (x - \alpha)g(x)$, where $g(x)$ in its turn has a root in L, etc., i.e. f factors into linear factors.

`Corollary.` *Every field F has an algebraically closed algebraic extension $\overline{F}$.*

`Proof:` Take $\overline{F} = \widehat{F} = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$.

`Lemma 2.` *Given an algebraic extension $E \supset F$, any embedding $\sigma : F \hookrightarrow L$ of F into an algebraically closed field L can be extended to an embedding $\tilde{\sigma} : E \hookrightarrow L$ (i.e. $\tilde{\sigma}|_F = \sigma$).*

`Proof.` We will find such an embedding by applying Zorn's lemma. Consider the set of pairs (F', σ'), where F' is an extension of F contained in E, and $\sigma' : F' \hookrightarrow L$ is an embedding such that $\sigma'|_F = \sigma$. Introduce partial ordering on the set of such pairs: $(F', \sigma') \leq (F'', \sigma'')$ if $F' \subset F''$ and $\sigma''|_{F'} = \sigma'$. Given a linearly ordered collection $\{(F^{(i)}, \sigma^{(i)})\}$ of such pairs, take $F^{(\infty)} := \cup_i F^{(i)}$ and define $\sigma^{(\infty)} : F^{(\infty)} \hookrightarrow L$ via $\sigma^{(\infty)}(\alpha) = \sigma^{(i)}(\alpha)$ where $F^{(i)} \ni \alpha$. Then $F^{(\infty)}$ is an extension of F contained in E, $\sigma^{(\infty)}$ is its embedding into L such that $\sigma^{(\infty)}|_F = \sigma$, and the pair $(F^{(\infty)}, \sigma^{(\infty)})$ is an upper bound for all $(F^{(i)}, \sigma^{(i)})$. By Zorn's lemma, there exists a maximal element $(\tilde{F}, \tilde{\sigma})$. We claim that $\tilde{F} = E$. Indeed, if $\alpha \in E$ is not in $\tilde{F}$, let $f = x^n + a_1 x^{n-1} + \cdots + a_n$ be the minimal polynomial of α in $\tilde{F}[x]$, and $g = x^n + \tilde{\sigma}(a_1)x^{n-1} + \cdots + \tilde{\sigma}(a_n)$. Let β be a root of g in L (this is where we need L to be algebraically closed). Then the embedding $\tilde{\sigma} : \tilde{F} \subset L$ can be extended to $\tilde{F}(\alpha)$ by mapping α to β. This contradicts the maximality of $(\tilde{F}, \tilde{\sigma})$, and shows that $\tilde{F} = E$.

`Remark.` Note that when $E \supset F$ is finite, the use of Zorn's lemma is unnecessary, since any tower of extensions of F in E stops after finitely many steps.

Applying now Lemma 2 to $L = \overline{F}$, $\sigma : F \subset \overline{F}$ the natural embedding, and $E = \overline{F}'$ another algebraically closed algebraic extension of F, we obtain an embedding $F \subset \tilde{\sigma}(\overline{F}') \subset \overline{F}$. Since $\sigma(\overline{F}') \cong \overline{F}'$ is algebraically closed, and $\overline{F}$ is algebraic over it, we conclude that $\sigma(\overline{F}') = \overline{F}$.

5. Finite fields. A finite field F must have finite characteristic p, i.e. be a finite extension of $\mathbb{Z}_p$, of certain degree $n = [F : \mathbb{Z}_p] < \infty$, and hence algebraic, consisting of $q := p^n$ elements. By Lemma 2, F can be embedded into the algebraic closure of $\mathbb{Z}_p$: $\overline{\mathbb{Z}_p} \supset F \supset \mathbb{Z}_p$. Below we describe all subfields in $\overline{\mathbb{Z}_p}$.

To begin with, every $\alpha \in \overline{\mathbb{Z}_p}$ is contained in a finite subfield $F = \mathbb{Z}_p(\alpha)$ of certain degree n over $\mathbb{Z}_p$. Since the multiplicative group $F^\times$ has order $p^n - 1$, all elements of F are roots of $x^{p^n} - x$. Since this polynomial cannot have more than p^n roots, we conclude that F can

be characterized in $\overline{\mathbb{Z}_p}$ as the set of all roots of this polynomial. To prove the converse, i.e. that for every $n = 1, 2, \dots$ the set of roots of $x^{p^n} - x$ forms a subfield in $\overline{\mathbb{Z}_p}$ of order p^n, consider the *Frobenius map*

$$\Phi : \overline{\mathbb{Z}_p} \to \overline{\mathbb{Z}_p} : \alpha \mapsto \alpha^p.$$

It follows from the properties of the binomial coefficients $\binom{p}{k} \equiv 0 \mod p$ for $k \neq 0, p$, that $\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta)$. It is also obvious that $\Phi(\alpha\beta) = \Phi(\alpha)\Phi(\beta)$. Since $\Phi(1) = 1$, Φ is an injective field homomorphism. But $\Phi(\overline{\mathbb{Z}_p}) \cong \overline{\mathbb{Z}_p}$ is algebraically closed, and so $\Phi(\overline{\mathbb{Z}_p}) = \overline{\mathbb{Z}_p}$, i.e. Φ is an *automorphsm* of $\overline{\mathbb{Z}_p}$ over $\mathbb{Z}_p$.

Note that *the roots of $x^{p^n} - x$ are fixed points of Φ^n.* Clearly, the sums, products, and ratios of fixed points of a field automorphism are also fixed points of it, and therefore form a subfield. It remains to show that the number of fixed points of Φ^n equals p^n, i.e. that $x^{p^n} - x$ (which must factor over $\overline{\mathbb{Z}_p}$ into p^n linear factors) has only simple roots. We'll prove this in the next section. Taking this for granted, we obtain

`Theorem.` *For each $n = 1, 2, \dots$, the field $\overline{\mathbb{Z}_p}$ contains a unique subfield F_{p^n} of order p^n, namely the set of fixed points of the nth power Φ^n of the Frobenius automorphism, and $\overline{\mathbb{Z}_p} = \cup_{n>0}\mathbb{F}_{p^n}$.*

`Corollary 1.` *For every prime p and every $n > 0$, a field of order p^n exists and is unique up to isomorphism.*

Indeed, such a field is algebraic over $\mathbb{Z}_p$, and therefore is contained in the algebraic closure of $\mathbb{Z}_p$, which is unique up to isomorphism.

`Corollary 2.` *$\mathbb{F}_{p^n}$ contains $\mathbb{F}_{p^m}$ if and only if $m|n$.*

The "only if" part follows from the fact that that a degree d extension of $\mathbb{F}_q$ has q^d elements. Conversely, when $n = md$, fixed points of Φ^m are fixed by Φ^{md} as well.

`Corollary 3.` *The mth power Φ^m of the Frobenius automorphism defines an automorphism of $\mathbb{F}_{p^{md}}$ over $\mathbb{F}_{p^m}$ (i.e. identical on $\mathbb{F}_{q^m}$), and generates the cyclic group of order d of such automorphism.*

We will see later that these are all automorphisms of $\mathbb{F}_{p^{md}}$ over $\mathbb{F}_{p^m}$.

Thus, the set of finite subfields in $\mathbb{F}_{p^\infty}$, partially ordered by inclusion, is in one-to-one correspondence with the set of positive integers $\mathbb{N} = \{1, 2, 3, \dots\}$ partially ordered by divisibility $m|n$, and with the set of subgroups $n\mathbb{Z}$ in $\mathbb{Z}$ ordered by the *inverse* inclusion. Namely, in the infinite cyclic group generated by Φ, to a field $\mathbb{Z}_{p^n}$ there corresponds the subgroup (generated by Φ^n) of those automorphisms which fix all elements of $\mathbb{F}_{p^n}$.

This picture may later serve us as an illustration to the Fundamental Theorem of Galois Theory.

6. Multiple roots. How to determine whether a polynomial has multiple roots?

Define the *derivative* $d/dx : F[x] \to F[x], f \mapsto f'$ as an F-linear map such that $d(x^n)/dx := nx^{n-1}$ for each $n = 0, 1, 2, \ldots$:

$$\frac{d}{dx}\left(a_0x^n + a_1x^{n-1} + \cdots + a_n\right) := a_0nx^{n-1} + a_1(n-1)x^{n-2} + \cdots + a_{n-1}.$$

It satisfies the *product* (or *Leibniz'*) rule: $(fg)' = f'g + fg'$. If a polynomial $f \in F[x]$, factored over $\overline{F}$ as $f(x) = c\prod_i(x - \alpha_i)$, has a double root α, then $f'(\alpha) = 0$, and hence f and f' are *not* coprime in $F[x]$. This can be detected by the Euclidean algorithm inside $F[x]$ without resorting to any extension of F.

For example, $f(x) := x^{p^n} - x$ from $\mathbb{Z}_p[x]$ has $f'(x) = p^n x^{p^n-1} - 1 = -1$, which is a unit in $F[x]$, and hence is coprime to f. Therefore $x^{p^n} - x$ has only simple roots, as assumed earlier.

Another question which can be resolved now is how the *inverse* to the Frobenius automorphism Φ of $\mathbb{F}_{p^\infty}$ is defined. For $\alpha \in \mathbb{F}_{p^\infty}$, we are looking for β such that $\beta^p = \alpha$, i.e. for a root of polynomial $g(x) := x^p - \alpha$ from $\mathbb{F}_{p^\infty}[x]$. What should be puzzling here is how can such β be unique? (But it should be, since Φ is bijective!)

We encounter here a phenomenon impossible in characteristic 0: $g'(x) = px^{p-1} = 0$ identically, as well as $g'' = 0$, $g''' = 0$, and so on. Thus, if $g(\beta) = 0$, then β should be a multiple root, of multiplicity equal to the degree n of g. And indeed: $(x - \beta)^p = x^p - \beta^p = x^p - \alpha$. Thus, $\Phi^{-1}(\alpha) = \beta$, the only (though multiple) root of $x^p - \alpha$.

7. Separability. Let's now explore the question whether an *irreducible* polynomial $f \in F[x]$ (which we will for convenience assume monic) of degree > 1 can have multiple roots. First, it is impossible when $\mathrm{char}(F) = 0$, since in this case f' is not constant and would have a non-trivial common factor with f, making f reducible. However, if $\mathrm{char}(F) = p$, it is possible that $f' = 0$ identically. This happens exactly when $f(x) = g(x^p)$, where $g \in F[y]$ is another polynomial — which in its turn may have or not have the same property $g' = 0$. In a few steps, we arrive at $f(x) = h(x^{p^e})$ where h is irreducible over F and has only simple roots. Factoring $h = \prod(x - \alpha_i)$ over $\overline{F}$, and taking β_i to be a root of $x^{p^e} - \alpha_i$ in $\overline{F}$, we find that $f(x) = \prod(x - \beta_i)^{p^e}$.

This exotic phenomenon is called "non-separability". More precisely, an element $\alpha \in \overline{F}$ whose minimal polynomial has only simple roots is called a *separable element*. An irreducible polynomial from $F[x]$

which has only simple roots in $\overline{F}$ is called a *separable polynomial*. An extension $K \supset F$ all of whose elements are separable over F is called *separable extension*. Otherwise the extension, or the polynomial, or the element are called *non-separable* (as for example each element β_i above).

Not that a field E separable over $F \subset E$ remains separable over any intermediate subfield K. Indeed, the minimal polynomial for $\alpha \in E$ over K divides the minimal polynomial of α over F, and if the latter has only simple roots, the former does too. (Of course, K is also separable over F — because it consists of separable elements.)

In the sequel, we will deal with only separable extensions.

A field F is called *perfect* if every irreducible polynomial from $F[x]$ is separable. Thus, all fields of characteristic 0 are perfect. Any algebraically closed field is perfect (just because all irreducibles over it have degree 1). Any algebraic extension $K \supset P$ of a perfect field P is perfect (because any algebraic extension field $L \supset K$ is algebraic over P, hence separable over P, and hence separable over K).

Besides, *any finite field is perfect*. Indeed, if f is irreducible of degree n in $\mathbb{F}_q[x]$, and α is a root of f, then α is a root of $g = x^{q^n} - x$. Since f is irreducible, and the greatest common divisor of it and g is non-trivial, we conclude that f divides g. But g has only simple roots, hence so does f.

8. Primitive elements.

`Theorem.` *Let $E \supset F$ be a finite separable extension. Then $E = F(\theta)$ for some $\theta \in E$, i.e. E is obtained by adjoining to F one element.*

It is called a *primitive element* of the extension.

`Proof.` Since E can be obtained by adjoining consecutively several elements to F, it suffices to prove the theorem for a field $F(\alpha, \beta)$ obtained by adjoining two algebraic elements. We may assume that F is infinite, since if its is not, then $F(a, \beta)$ is finite too, and therefore its multiplicative group is cyclic (as is the multiplicative group of any finite filed), and so its generator can be taken on the role of a primitive element.

Let f and g be minimal polynomials for α and β, and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be roots of f in $\overline{F}$, and and $\beta_1 = \beta, \beta_2, \ldots, \beta_m$ of g (distinct due to the separability assumption). Each linear equation $\alpha_i + x\beta_j = \alpha + x\beta$ with $j > 1$ has at most one root in F (since $b_j \neq \beta$), and so there exists $c \in F$ such that $\alpha_i + c\beta_j \neq \alpha + c\beta$ for all i, j with $j \neq 1$. We will show that $\theta := \alpha + c\beta$ is primitive. Indeed, β is a common root of two polynomial equations with coefficients in $F(\theta)$:

$g(x)$ and $f(\theta - cx)$. Other roots of g are β_j with $j > 1$, and do not satisfy $f(\theta - c\beta_j) = 0$ since $\alpha + c\beta - c\beta_j \neq \alpha_i$ for any i. Therefore the greatest common divisor of these polynomials (which by the Euclidean algorithm must have coefficients in $F(\theta)$) is $x - \beta$. Thus, $\beta \in F(\theta)$, and hence $\alpha = \theta - c\beta \in F(\theta)$ too, and so $F(\alpha, \beta) = F(\theta)$.

`Corollary 1.` *A separable extension $E \supset F$ of finite degree n has exactly n embeddings into $\overline{F}$.*

`Proof.` Let $h \in F[x]$ be the minimal polynomial of a primitive element θ of E over F, and $\theta_1 = \theta, \theta_2, \dots, \theta_n$ be its roots. Here $n = \deg h$ due to separability. By the Key Lemma, $E = F(\theta) \cong F[x]/(h)$ has n embeddings into $\overline{F}$ over F: Every such an embedding $E \subset \overline{F}$ is uniquely determined by a root θ_i to which θ is mapped.

`Corollary 2.` *In the group of automorphisms of $\overline{F}$ over F, the subgroup of automorphisms identical on an intermediate subfield $E \subset F$, separable and finite over F, has finite index $[E : F]$.*

`Proof.` By Lemma 2 of Section 4, applied to the extension $E \subset \overline{F}$, any re-embedding of E into $\overline{F}$ extends to an automorphism of $\overline{F}$. Therefore automorphisms of $\overline{F}$ over F act transitively on the set of such re-embedding of $E \subset \overline{F}$ identical on F. By Corollary 1, there are $[E : F]$ of them. The stabilizer consists of those automorphisms which preserve the primitive element θ, and hence are identical on $E = F(\theta)$.

9. Normality. Elements $\alpha, \beta \in \overline{F}$ are called *conjugated* over F is they are transformed into each other by an automorphism of $\overline{F}$. We see from Lemma 2 of Section 4, that α is conjugated exactly to each of the n roots of its minimal polynomial, where n is equal to the degree of this polynomial, *provided that it is separable*, i.e. has no multiple roots.

Given a polynomial $f \in F[x]$, irreducible or not, (or any set of polynomials), consider in $\overline{F}$ the smallest subfield containing all roots $\alpha_1, \alpha_2, \dots$ of f (respectively, all roots of the polynomials from the set). This field can be obtained by consecutively adjoining the roots to F, resulting in the field $F(\alpha_1, \alpha_2, \dots)$, or alternatively, by intersecting all subfields in $\overline{F}$ containing all α_i. The field $F(\alpha_1, \alpha_2, \dots)$ is called the *splitting field* of f (respectively, of the given set of polynomials).

`Proposition.` *The following conditions for a subfield $E \subset \overline{F}$ containing F are equivalent:*

(i) E is a splitting field of a set (possibly infinite) of polynomials from $F[x]$.

(ii) E is invariant under all automorphisms of $\overline{F}$ over F (i.e. automorphisms identical on F).
(iii) Every irreducible polynomial $g \in F[x]$ which has a root in E has all its roots in E.

`Proof.` (i) implies (ii): Any automorphism of $\overline{F}$ over F preserves each polynomial from $F[x]$, and hence merely permutes the roots of it in $\overline{F}$, and hence preserves the smallest subfield containing the roots of the given set of polynomials.
(ii) implies (iii): Since all roots of g are conjugated by automorphisms of $\overline{F}$, if one of them lies in E, all others lie there too.
(iii) implies (i): For any collection of generators of E over F, take the minimal polynomial over F of each generator. Then E is the splitting field for this collection of polynomials.

An algebraic extension $E \supset F$ satisfying any (and hence all) of the three conditions is called *normal*.

`Corollary.` *In the group of automorphisms of $\overline{F}$ over F, the automorphisms identical on a subfield E, normal over F, form a normal subgroup.*

`Proof.` This subgroup is the kernel of the group homomorphism which to an automorphism of $\overline{F}$ over F associates an automorphism of E over F, defined by restricting the former to the subfield E (invariant due to the normality assumption).

Note that if E is normal over F, it remains normal over every intermediate subfield, $E \supset K \supset F$, since every automorphism of $\overline{F} = \overline{K}$ identical on K is also identical on F, and thus leaves E invariant.

10. Galois groups. Let $E \supset F$ be a finite, separable, normal extension. Automorphisms of E identical on F form a group, which is called the *Galois group* of the extension, and is denoted $G(E/F)$. By the previous results, it is a finite group of order $[E : F]$, and can be identified with the quotient of the group of automorphisms of $\overline{F}$ over F by the normal subgroup of those automorphisms which are identical on E.

`The Fundamental Theorem of Galois Theory.` *For a separable, normal, finite field extension $E \supset F$, there is a bijection between the set of subgroups $H \subset G$ in the Galois group $G = G(E/F)$ and the set of intermediate fields $E \supset K \supset F$, reverse with respect to the partial*

orderings of these sets by inclusion, and defined by

$$H \mapsto K = E^H := \{\alpha \in E \mid \forall h \in H,\ h(\alpha) = \alpha\}$$
$$K \mapsto H = G_K := \{h \in G \mid \forall \alpha \in K,\ h(\alpha) = \alpha\}.$$

Furthermore, $G_K = G(E/K)$, so $|G_K| = [E : K]$, $|G/G_K| = [K : F]$. Moreover, conjugated subgroups H correspond to conjugate subfields E^H, and in particular the subfield E^H is normal if and only if H is normal in G. When this is the case, the quotient group $G/H = G(E^H/F)$.

`Proof.` Obviously, all elements in E invariant under transformations from $H \subset G$ form a subfield, E^H, and conversely, the transformations of E over F identical on K form a subgroup, G_K. It is also clear that $K \subset K'$ implies $G_{K'} \supset G_K$, and $H \subset H'$ implies $E^H \supset E^{H'}$.

Suppose that all elements of G_K fix some $\alpha \in E$. Then α has only one conjugate element in the normal separable extension $E \supset K$. Then the degree of the minimal polynomial of α over K is equal to 1, i.e. $\alpha \in K$. Thus, $E^{G_K} = K$.

Consider now the subfield E^H of fixed points of some subgroup $H \subset G$. The extension $E \supset E^H$ is generated by some primitive element θ, which is a root of the polynomial $\prod_{h\in H}(x - h(\theta))$. The polynomial is H-invariant, and hence lies in $E^H[x]$. The degree $[E : E^H]$ cannot exceed therefore the degree $|H|$ of this polynomial. But the degree equals the order of the Galois group $G(E/E^H) = G_{E^H} \supset H$ of this extension. Thus, $H = G_{E^H}$ is the Galois group, and consequently, the two correspondences: $H \mapsto E^H$ and $K \mapsto G_K$, are inverse to each other.

Elements $g \in G$ from the same left H-coset transform E^H to the same subfield, $g(E^H)$, conjugate to E^H, whose group $G^{g(E^H)} = gHg^{-1}$, i.e. is conjugated to H. Thus, H is normal in G whenever E^H is G-invariant, i.e. normal over F. When it is, the homomorphism $G \to G(E^H/F)$, defined by the restriction of $g \in G$ to E^H, has H as its kernel, and is surjective, because $|G(E^H/F)| = [E^H : F] = [E : F]/[E : E^H] = |G|/|H|$. Thus, $G(E^H/F) = G/H$.

`Example.` Each extensions $\mathbb{F}_{p^n} \supset \mathbb{Z}_p$ is normal and separable, since $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$, whose roots are simple, and of which $\mathbb{F}_{p^n}$ consists. Therefore $\mathbb{F}_{p^{md}} \supset \mathbb{F}_{p^m}$ is also normal and separable, and has Galois group of order d. But this Galois group contains the cyclic subgroup of order d generated by Φ^m. Thus this cyclic group is the entire Galois group of this extension.

Remark. Let $f \in F[x]$ be the minimal polynomial of a primitive element θ in a normal separable extension $E \supset F$ of degree n. Then

the Galois group permutes the n roots of the minimal polynomial, and is thereby realized as a subgroup of order n in S_n.

11. Cyclotomic fields. Let n be a positive integer. The nth *cyclotomic polynomial* is defined by

$$\psi_n(x) := \prod_{k \in \mathbb{Z}_n^\times} \left(x - e^{2\pi i k/n}\right),$$

i.e. as the monic polynomial of degree $\varphi(n) := |\mathbb{Z}_n^\times|$ whose roots are all the primitive complex n-th roots of unity. Since each root of $x^n - 1$ (i.e. each nth root of unity ζ) is primitive dth root of unity for some divisor $d|n$ (namely, d is the least power such that $\zeta^d = 1$), we have

$$x^n - 1 = \prod_{\zeta : \zeta^n = 1} (x - \zeta) = \prod_{d|n} \psi_d(x).$$

Since $x^n - 1 \in \mathbb{Z}[x]$, it follows by induction that all $\psi_n \in \mathbb{Z}[x]$. Indeed, $\psi_1 = x - 1 \in \mathbb{Z}[x]$, and if $\psi_d \in \mathbb{Z}[x]$ for all $d < n$, then

$$\psi_n(x) = (x^n - 1) / \prod_{d|n, d<n} \psi_d(x) \in \mathbb{Z}[x],$$

because the long division algorithm of an integer coeficient pollynomial by a monic integer coefficient polynomial is performed within $\mathbb{Z}[x]$.

`Examples.`

$$x^6 - 1 = \psi_1\psi_2\psi_3\psi_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1),$$
$$x^8 - 1 = \psi_1\psi_2\psi_4\psi_8 = (x-1)(x+1)(x^2+1)(x^4+1).$$

`Theorem.` *Cyclotomic polynomials are irreducible over* $\mathbb{Q}$.

`Proof.` We want to show that the minimal polynomial for $e^{2\pi i/n}$ must also have $e^{2\pi i k/n}$ as a root provided that k is coprime to n. Since such k can be written as a product of primes coprime to n, it suffices to show that if ζ is an nth root of unity, and a prime p does not divide n, then ζ and ζ^p are conjugate over $\mathbb{Q}$.

Thus, let f be the minimal polynomial for ζ, and hence $x^n - 1 = f(x)g(x)$ for some $g \in \mathbb{Z}[x]$. If ζ^p is *not* a root of f, then it is a root of g, and hence ζ is a root of $g(x^p)$. From irreducibility of f we conclude that f divides $g(x^p)$ over $\mathbb{Z}$.

Now denote by $\widehat{f}$ and $\widehat{g}$ the reductions of f and g modulo p. Since $\widehat{g}(x^p) = (\widehat{g}(x))^p$ in $\mathbb{Z}_p[x]$, we conclude that $\widehat{f}$ and $\widehat{g}$ have a common root in $\overline{\mathbb{Z}_p}$. This implies that $x^n - 1 = \widehat{f}(x)\widehat{g}(x)$ has a multiple root in $\overline{\mathbb{Z}_p}$. But since p does not divide n, the only root of the derivative nx^{n-1} is

$x = 0$, which is not a root of $x^n - 1$. This contradiction show that ζ^p must be a root of f, as required.

`Corollary 1.` *The field $\mathbb{Q}\left(e^{2\pi i/n}\right)$ is the splitting field of the nth cyclotomic polynomial ψ_n, and is therefore a normal extension of $\mathbb{Q}$ of degree $\varphi(n) = |\mathbb{Z}^\times|$.*

The field $\mathbb{Q}\left(e^{2\pi i/n}\right)$ is called the nth *cyclotomic field*.

`Corollary 2.` *The Galois group of the nth cyclotomic field over $\mathbb{Q}$ is isomorphic to the multiplicative group $\mathbb{Z}_n^\times$.*

`Proof.` Every automorphism of this field maps $e^{2\pi i/n}$ into another primitive nth root of unity, $e^{2\pi ik/n}$, where k is coprime to n, and is uniquely determined by a choice of such a root. Let σ_k be the automorphism, determined by the choice of such k (which is relevant only modulo n). We have:

$$\sigma_k\sigma_l\left(e^{2\pi i/n}\right) = \sigma_k\left(e^{2\pi il/n}\right) = e^{2\pi ilk/n} = \sigma_{kl}\left(e^{2\pi i/n}\right),$$

i.e. $\sigma_k\sigma_l = \sigma_{kl}$.

`Example 1.` The 8th cyclotomic polynomial $\psi_8 = x^4 + 1$ has roots $\zeta^{\pm 1} = (1 \pm i)/\sqrt{2}$ and $\zeta^{\mp 3} = -(1 \pm i)/\sqrt{2}$. The cyclotomic field is

$$\mathbb{Q}(\zeta) = \{a + b\zeta + c\zeta^2 + d\zeta^3 \mid a, b, c, d \in \mathbb{Q},\ \zeta^4 = -1\}.$$

Its Galois group, isomorphic to $\mathbb{Z}_8^\times = \{\pm 1, \pm 3 \mod 8\}$, has 3 subgroup of order 2, generated by σ_k, $k = -1, 3, -3 \mod 8$ respectively. Thus, the field has 3 non-trivial subfields, each a degree 2 extensions of $\mathbb{Q}$ formed by the fixed points of σ_k.

For $k = -1$, we have:

$$\sigma_{-1} : a + b\zeta + c\zeta^2 + d\zeta^3 \mapsto a - b\zeta^3 - c\zeta^2 - d\zeta,$$

i.e. the fixed points are characterized by $b = -d$, $c = 0$, and have the form $a + b(\zeta - \zeta^3) = a + b\sqrt{2}$. The subfield is therefore $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2 - 2)$.

For $k = 3$ we similarly have

$$\sigma_3 : a + b\zeta + c\zeta^2 + d\zeta^3 \mapsto a + b\zeta^3 - c\zeta^2 + d\zeta.$$

So, the fixed points have the form $a + b(\zeta + \zeta^3) = a + b\sqrt{2}i$, i.e. the subfield is $\mathbb{Q}[\sqrt{2}i] = \mathbb{Q}[x]/(x^2 + 2)$.

Finally, for $k = -3$ we have

$$\sigma_{-3} : a + b\zeta + c\zeta^2 + d\zeta^3 \mapsto a - b\zeta + c\zeta^2 - d\zeta^3.$$

So, the fixed points $a + b\zeta^2 = a + bi$ form the cyclotomic subfield $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2 + 1)$.

`Example 2.` Take $n = p$ prime. All roots of $\psi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ can be obtained from $\zeta = e^{2\pi i/p}$ by the action of the Galois group $\cong \mathbb{Z}_p^\times$, which is cyclic of order $p-1$ (since the multiplicative groups of any finite field is cyclic). Let $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ denote a generator of this cyclic group. Then iterations of σ as a permutation of the roots arranges all the $p-1$ roots into a cycle of length $p-1$, staring from ζ:

$$\sigma : \zeta \mapsto \sigma(\zeta) \mapsto \sigma^2(\zeta) \mapsto \cdots \mapsto \sigma^{p-2}(\zeta)[\mapsto \sigma^{p-1}(\zeta) = \zeta].$$

The roots $\sigma^r(\zeta)$, $r = 1, \ldots, p-1$, form a basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.

Indeed, these are just permuted $\zeta^j, j = 1, \ldots, p-1$. Any non-trivial linear relation $\sum a_j \zeta^j = 0$ between them with rational coefficients a_j would yield, after dividing by ζ, a polynomial $\sum a_j x^{j-1}$ of degree $< \deg \psi_p$ with a root ζ. But this contradicts the minimality of ψ_p.

Now the subfield of $\mathbb{Q}(\zeta)$ whose elements are fixed by the cyclic group of σ^d, where d is any divisor of $p-1$, can be described as the span of the following *Gauss sums*:

$$\sum_{m=1}^{(p-1)/d} \sigma^{r+md}(\zeta), \quad r = 1, \ldots, d.$$

12. Regular polygons. The ancient problem about (the possibility of) constructing a regular n-gon by straightedge and compass was solved by K. F. Gauss around 1800. The problem naturally leads to studying cyclotomic fields. Namely, if the unit circle is divided into n equal parts, then $\cos 2\pi/n$ and $\sin 2\pi/n$ can be obtained by a succession of quadratic extensions of $\mathbb{Q}$, and hence $\zeta = e^{2\pi i/n}$ (obtained by adjoining $\sqrt{-1}$), together with the whole cyclotomic field $\mathbb{Q}(\zeta)$ can be obtained by such a succession. Conversely, if $\mathbb{Q}(\zeta)$ is obtained by a succession of quadratic extensions of $\mathbb{Q}$, then $\cos 2\pi/n = (\zeta + \zeta^{-1})/2$ and $\sin 2\pi/n = \sqrt{1 - \cos^2 2\pi/n}$ are constructible.

Suppose therefore that $\mathbb{Q}\left(e^{2\pi i/n}\right) \subset K$ where the field K is obtained by a succession of quadratic extensions of $\mathbb{Q}$. Then the degree $[K : \mathbb{Q}]$ must be a power of 2, and therefore the degree $\varphi(n)$ of the cyclotomic extension must be a divisor of it, i.e. a power of 2 as well.

`Proposition.` *For $n = p_1^{k_1} \cdots p_r^{k_r}$, where p_i are distinct primes, and $k_i > 0$, we have the following explicit formula:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \prod_{i=1}^{r} (p_i - 1) p_i^{k_i - 1}.$$

`Proof.` Consider the ring homomorphism

$$\mathbb{Z}/n\mathbb{Z} \to \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right),$$

defined by assigning to a congruence class modulo n the string of its congruence classes modulo $p_i^{k_i}$. Since the latter powers are pairwise coprime, the kernel of the homomorphism is trivial. But the order of both rings is the same, equal to n, and so the map must be a ring isomorphism. In particular, it establishes an isomorphism between the groups of units:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times.$$

This implies $\varphi(n) = \prod_i \varphi(p_i^{k_i})$. It remains to notice that out of p^k remainders modulo p^k, p^{k-1} are divisible by p, so $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$.

We see that $\varphi(n)$ is a power of 2 only if n is a power of 2 or the product of such a power with one or several *distinct* odd primes of the form $p = 2^m + 1$. Furthermore, note that for an odd l, $x^l + 1$ is divisible by $x + 1$. Therefore if the above m has an odd factor, then $p^m + 1$ is composite. Thus, p must be a *prime of the form* $2^{2^k} + 1$.

The numbers $F_k = 2^{2^k} + 1$ (called *Fermat's numbers*, because P. Fermat conjectured that they all are primes) are known to be primes for $k = 0, 1, 2, 3, 4$:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537.$$

F_5 is actually composite (divisible by 641), and it is currently not known whether any of the other Fermat numbers is prime.

On the other hand, when $p = 2^{2^k} + 1$ is prime, then the cyclotomic field $\mathbb{Q}\left(e^{2\pi i/p}\right)$ is obtained from $\mathbb{Q}$ by a succession of quadratic extensions.

Indeed, the multiplicative group $(\mathbb{Z}_p)^\times$ is *cyclic* (as it is for any finite field) of order 2^{2^k}. Therefore the Galois group G has a chain of nested cyclic subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{2^k} = \{\mathrm{id}\}$, with G_s of index 2 in G_{s-1}. Respectively, the cyclotomic field has a chain of nested subfields $\mathbb{Q} = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_{2^k} = \mathbb{Q}\left(e^{2\pi i/p}\right)$, where each degree $[E_s : E_{s-1}] = 2$.

Clearly, if m and n are coprime, once a circle is divided into m equal parts and n equal parts, it is also divided into mn equal parts (e.g. because $1/mn = k/n + l/m$ for some k and l). Since bisecting any angle is easily accomplished by straightedge and compass, we arrive at the following

`Theorem` (Gauss). *A regular n-gon can be constructed by straightedge and compass if and only if n is a power of 2 or the product of a power of 2 with one or several distinct Fermat primes.*

`Example.` Prior to establishing this theorem, Gauss invented a construction of the regular 17-gon. Thus, take $p = 17 = 2^{2^2} + 1$. The multiplicative group $\mathbb{Z}_{17}^\times$ is cyclic of order 16, with 8 generators, one of which is 3: $3^2 \equiv (-8) \mod 17$, $3^4 \equiv (-8)^2 \equiv (-4) \mod 17$, $3^8 \equiv (-4)^2 \equiv (-1) \mod 17$, and only $3^{16} \equiv 1 \mod 17$. Therefore the automorphism of $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/17}$, defined by $\sigma(\zeta) = \zeta^3$ generates the Galois group G_0. The subgroups G_1, G_2, and G_3 are generated respectively by $\sigma^2(\zeta) = \zeta^{-8}$, $\sigma^4(\zeta) = \zeta^{-4}$, and $\sigma^8(\zeta) = \zeta^{-1}$.

Iterating σ, we get all the 16 roots $\zeta^j, j \in (\mathbb{Z}/17\mathbb{Z})^\times$ of ψ_{17} in this order:

$$\zeta^1, \zeta^3, \zeta^{-8}, \zeta^{-7}, \zeta^{-4}, \zeta^5, \zeta^{-2}, \zeta^{-6}, \zeta^{-1}, \zeta^{-3}, \zeta^8, \zeta^7, \zeta^4, \zeta^{-5}, \zeta^2, \zeta^6 \ [, \zeta^1].$$

Therefore fixed points of σ^2 form the subspace spanned by 2 Gauss sums

$$\eta_+ = \sum_{j=1,2,4,8} (\zeta^j + \zeta^{-j}), \text{ and } \eta_- = \sum_{j=3,5,6,7} (\zeta^j + \zeta^{-j}).$$

Note that both $\eta_+ + \eta_-$ and $\eta_+\eta_-$ are σ-invariant, and hence lie in $\mathbb{Q}$, making $\eta_\pm$ the roots of a quadratic equation. Explicitly, $\eta_+ + \eta_- = -1$, and (as one can compute) $\eta_+\eta_- = 4(\eta_+ + \eta_-) = -4$. So the quadratic equation is

$$x^2 + x - 4 = 0, \quad \text{i.e. } \eta_\pm = \frac{-1 \pm \sqrt{17}}{2}.$$

Next, fixed points of σ^4 form the subspace spanned by 4 Gauss sums

$$\lambda_1 = \mu_1 + \mu_4, \ \lambda_2 = \mu_2 + \mu_8, \ \lambda_3 = \mu_3 + \mu_5, \ \lambda_4 = \mu_6 + \mu_7,$$

where $\mu_j := \zeta^j + \zeta^{-j} = 2\cos 2\pi j/17$.

Note that $\lambda_1 + \lambda_2 = \eta_+$, $\lambda_3 + \lambda_4 = \eta_-$, $\lambda_1\lambda_2 = -1 = \lambda_3\lambda_4$. Thus, $\lambda_{1,2}$ and $\lambda_{3,4}$ are respectively the roots of the quadratic equations

$$x^2 - \eta_+ x - 1 = 0 \ \text{ and } \ x^2 - \eta_- x - 1 = 0.$$

Finally, fixed points of σ^8 form the subspace spanned by 8 Gauss sums $\mu_j, j = 1, 3, 8, 7, 4, 5, 2, 6$. It is not hard to see that this field is $\mathbb{Q}(\cos 2\pi/17)$, i.e. μ_1 is its primitive element over $\mathbb{Q}$. We have: $\mu_1 + \mu_4 = \lambda_1$ and $\mu_1\mu_4 = \lambda_3$. Therefore μ_1, μ_4 can be found as the roots of the quadratic equation

$$x^2 - \lambda_1 x + \lambda_3 = 0.$$

This leads to an algorithm for constructing $\cos 2\pi/17$ by straightedge and compass.

13. Cyclic extensions. Finding the roots of quadratic polynomials $x^2 + ax + b$ is reduced to the operation of extracting square roots of given numbers thanks to the *quadratic formula*:

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

It is a classical problem of algebra to find out whether roots of a degree n polynomial

$$P(x) := x^n + a_1 x^{n-1} + \cdots + a_n$$

can be obtained by a succession of arithmetic operations and the operations of extracting mth roots (with arbitrary m) of previously computed numbers. The problem can be understood as the question about existence of a general formula for the roots of all degree n polynomials, but also makes sense for a particular polynomial whose coefficients are given explicitly.

The version concerning the general formula (say, for complex coefficient polynomials) can be interpreted in terms of the theory of fields by starting with the field $F = \mathbb{C}(a_1, \ldots, a_n)$ of all rational functions in the variables $a_1, \ldots, a_n$, and examining towers of algebraic extensions $F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_N$ such that each F_s is obtained from F_{s-1} by adjoining a root of certain order of one of its elements: $F_{s-1}(\sqrt[m]{\alpha})$, where $\alpha \in F_{s-1}$. The version of the problem concerning a specific root β of a specific polynomial P can also be phrased this way. Namely, one assumes that F_0 is a field containing all coefficients of P as well as all roots of unity, and tries to find a tower of extensions $F_s = F_{s-1}(\sqrt[m_s]{a_{s-1}})$ such that F_N contains β. In this case one says that β is *expressible in radicals*.

In any case, the problem requires a good understanding of splitting fields of polynomials $x^m - a$.

Let F be a field containing mth roots of unity ζ^k, $k = 1, \ldots, m-1$. For the sake of simplicity, let's assume that $\operatorname{char} F = 0$. Let a be any element of F, and α a root of $x^m - a$ in $\overline{F}$ (where $a \neq 0$). Then $\alpha, \zeta\alpha, \ldots, \zeta^{m-1}\alpha$ form a complete set of roots of $x^m - a$. This proves that $F(\alpha)$ is the splitting field of $x^m - a$ and is therefore normal. Any transformation from the Galois group of $F(\alpha)$ over F maps α to $\alpha\zeta^k$ an is determined by k modulo m. The composition of transformations $\alpha \mapsto \alpha\zeta^k$ and $\alpha \mapsto \alpha\zeta^l$ maps α to $\alpha\zeta^{k+l}$. This identifies the whole Galois group with a subgroup of the cyclic group of all mth roots of unity, and any such a subgroup is cyclic.

A normal separable extension with a cyclic Galois group is called *cyclic*. Thus, the extension $F(\sqrt[n]{a}) \supset F$ is cyclic. In the case when

$x^m - a$ is irreducible in $F[x]$, the Galois group has order m, and is identified with the entire cyclic group of the mth roots of unity. Our goal now is to prove that converse statement:

`Proposition.` *A normal extension $E \supset F$ with $G(E/F) \cong \mathbb{Z}_m$ of a characteristic 0 field F containing all mth roots of unity is obtained from F by adjoining a root of $x^m - a$ for some $a \in F$.*

`Proof.` Let σ be a generator of the Galois group $\cong \mathbb{Z}_m$. It can be considered as a linear transformation of the m-dimensional F-vector space E, satisfying $\sigma^m = I$. In particular, the eigenvalues of σ must be mth roots of unity. Since all of them lie in F, the space E can be decomposed into the direct sum of eigenspaces. Explicitly, for any $\beta \in E$, the *Lagrange resolvent*

$$\beta_l = \sum_{k=0}^{m-1} \zeta^{-kl} \sigma^k(\beta)$$

satisfies $\sigma(\beta_l) = \zeta^l \beta_l$, i.e. β_l, if non-zero, is an eigenvector of σ with the eigenvalue ζ^l. On the other hand, $\beta = (\beta_0 + \cdots + \beta_{l-1})/m$. Indeed, for a fixed k

$$\sum_{l=0}^{m-1} \zeta^{-kl} = \frac{1 - \zeta^{-km}}{1 - \zeta^{-k}} = 0 \text{ when } k = 1, \ldots, m-1,$$

and $= m$ when $k = 0$.

This is true for any linear transformation σ of finite order m, and the total dimension m can be split between those of the eigenspaces arbitrarily. It turns out that when σ is a field automorphism, all the eigenspaces have the same dimension 1. In particular, there exists $\beta \in E$ such that its Lagrange resolvent $\alpha := \beta_1 \neq 0$. Taking this for granted, we find that α^l, $l = 1, \ldots, m$, are eigenvectors of σ with the eigenvalues ζ^l. In particular, $a := \alpha^m$ lies in F (since it is fixed by σ), and α generates the whole extension (since it is not fixed by any non-trivial element of the Galois group). Thus $E = F(\alpha)$ where $\alpha^m = a \in F$.

A proof of the statement we took for granted makes use of the following fruitful idea: A field automorphism $E \to E$ defines a group homomorphism $E^\times \to E^\times$. In general, a homomorphism of a group G to the multiplicative group $K^\times$ of a field K is called a K-*character* of G. The following lemma about linear independence of different characters implies that $\sum_{k=0}^{m-1} \zeta^{-k} \sigma^k$ (considered as a linear combination of such characters σ^k with the coefficients ζ^{-k}) is non-zero, and hence there exists $\beta \neq 0$ such that $\beta_1 \neq 0$.

`Lemma` (E. Artin). *Different characters $\chi_1, \dots, \chi_n : G \to K^\times$ are linearly independent.*

`Proof.` Since $\chi(e) = 1$, the case of $n = 1$ is clear. Let $n > 1$, and

$$G \ni g \ \mapsto c_1\chi_1(g) + c_2\chi_2(g) + \dots + c_n\chi_n(g) = 0$$

be the shortest identically zero linear combination with non-zero coefficients c_i of different characters χ_i. Pick $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_2(g_0)$, and use he homomorphism property $\chi_i(g_0 g) = \chi_i(g_0)\chi_i(g)$ to rewrite the relation as

$$c_1\chi_1(g_0)\chi_1(g) + c_2\chi_2(g_0)\chi_2(g) + \dots + c_n\chi_n(g_0)\chi(g) = 0 \text{ for all } g \in G.$$

Subtracting from it the original relation multiplied by $\chi_1(g_0)$, we obtain a zero linear combination of $\chi_2, \dots, \chi_n$ where χ_2 occurs with the coefficient $c_2(\chi_2(g_0) - \chi_1(g_0)) \neq 0$. It is shorter than the initial one, which contradicts its choice, thus completing the proof.

14. Solvability by radicals. Let F be a field, which we still consider having characteristic 0 and containing all roots of unity of all relevant orders, and $\alpha \in \overline{F}$. We want to translate the property of α to be expressible in radicals into the language of Galois groups. For this, we need a notion from group theory: A finite group G is called *solvable* if it has a filtration by a chain of subgroups

$$G = G_0 \supset G_1 \supset \dots \supset G_N \supset \{e\}$$

such that each G_s is normal in G_{s-1}, and each quotient G_{s-1}/G_s is cyclic. Due to the properties of finite abelian groups, the last condition can be replaced by the equivalent (yet seemingly weaker) requirement that the quotients are abelian, or by the (seemingly stronger) one that they are cyclic of prime orders.

`Proposition.` *An element $\alpha \in \overline{F}$ is expressible in radicals if and only if it is contained in a normal extension $E \supset F$ whose Galois group $G(E/F)$ is solvable.*

`Proof.` There is one technical difficulty that we need to handle first. The same way as for nested $G \supset G' \supset G''$, G' being normal in G, and G'' in G' does *not* imply that G'' is normal in G, in a tower $F \subset F' \subset F''$ of fields extensions, F'' can be not normal over F even if it is normal over F', and F' is normal over F. For example, $\mathbb{Q}(\sqrt[4]{2})$ is not normal (since it does not contain the non-real roots of the minimal polynomial $x^4 - 2$) while each "floor" in the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ is normal.

Consider however a tower of extensions $F \subset E \subset E\,(\sqrt[p]{a}) \subset K$, where E is normal over F, $\sqrt[p]{a}$ is a root of prime order from some $a \in E$, and K is the smallest extension of $E\,(\sqrt[p]{a})$, normal *over* F. We

claim that if elements of E are expressible in radicals (starting from elements of F), then elements of K are also expressible in radicals. Indeed, if $\alpha = \sqrt[p]{a}$ is a root of $x^p - a$, then its conjugates $\sigma(\alpha) \in K$ by all elements $\sigma \in G(K/F)$ are roots of $x^p - \sigma(a)$, whose coefficient $\sigma(a) \in E$ (since E is normal), and by the assumption is expressible in radicals over F. Adjoining all $\sigma(\alpha)$ to E, we obtain a field contained in K and normal over F, since it is invariant under the entire Galois group $G(K/F)$. Thus, this field coincides with K, whose elements are therefore expressible in radicals. The moral is: we need to adjoin not only the root $\sqrt[p]{a}$, but also such roots of all elements conjugate to a.

Now we can conclude that any $\alpha \in \overline{F}$ expressible in radicals lies in some *normal over* F extension field E obtained from F by a succession of cyclic extensions, whose orders can be always assumed prime: $F = F_0 \subset F_1 \subset \cdots \subset F_N = E$. Therefore the Galois group $G(E/F)$ is filtered by the subgroups

$$G_s = \{\sigma \in G(E/F) \mid \sigma(a) = a \text{ for all } a \in F_s\},$$

each G_s normal in G_{s-1}, and such that G_{s-1}/G_s is cyclic (of prime order). Thus, $G(E/F)$ is solvable.

Conversely, when $G(E/F)$ is filtered by subgroups G_s with such properties, the fields F_s formed by fixed elements of G_s turn out to be cyclic extensions of F_{s-1} of prime orders, i.e. (by the results of the previous section) are obtained by adjoining to F_{s-1} a root $\sqrt[p]{a}$ for some $a \in F_{s-1}$. Thus, all elements of E are expressible in radicals.

Consider the relation

$$(x - x_1) \cdots (x - x_n) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

From it, the coefficients a_k of the polynomial on the right side are expressed as *elementary symmetric functions* of the roots $x_1, \ldots, x_n$ on the left:

$$\begin{aligned}
a_1 &= -(x_1 + \cdots + x_n) \\
a_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\
&\cdots \\
a_k &= (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k} \\
&\cdots \\
a_n &= (-1)^n x_1 \cdots x_n.
\end{aligned}$$

We apply the previous result to the field E of rational functions $\mathbb{C}(x_1, \ldots, x_n)$ with coefficients in the field $\mathbb{C}$ of complex numbers (or in any other field of characteristic 0 containing all roots of unity). Take

$F = \mathbb{C}(a_1, \dots, a_n)$ to be the subfield of it consisting of rational functions of the elementary symmetric functions $a_k(x_1, \dots, x_n)$, $k = 1, \dots, n$. Then $E \supset F$ is a normal algebraic extension: the splitting field of the polynomial $x^n + a_1 x^{n-1} + \dots + a_n \in F[x]$. The Galois group $G(E/F)$ is the total symmetric group S_n acting on E by the permutations of $x_1, \dots, x_n$. We arrive at the following

`Theorem` (Abel). *For $n > 4$, the roots x_i of the general equation $x^n + a_1 x^{n-1} + \dots + a_n$ of degree n are not expressible by radicals in terms of its coefficients a_k.*

`Proof.` For $n > 4$, the group S_n has only one non-trivial normal subgroup, A_n, which is simple, and non-cyclic. Thus, S_n is not solvable.

15. Cubics and quartics. To simplify computations, reduce the general cubic polynomial $x^3 + a_1 x^2 + a_2 x + a_3$ by "completing cubes", i.e. by translating $x \mapsto x - a_1/3$, to the cubic polynomial with the zero root sum: $x^3 + px + q$. It has 3 roots x_1, x_2, x_3 satisfying

$$x_1 + x_2 + x_3 = 0,\ x_1x_2 + x_2x_3 + x_3x_1 = p,\ x_1x_2x_3 = -q.$$

The filtration $S_3 \supset A_3 \supset \{e\}$ by the subgroup A_3 of order 3 and index 2 corresponds to the tower of extensions $F = \mathbb{C}(p, q) \subset F(\sqrt{D}) \subset F(x_1, x_2, x_3) = E$ of degree 2 and 3 respectively, where

$$\sqrt{D} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3),$$

is the Vandermonde determinant, invariant under A_3, but changing sign under odd permutations. Its square D, called the *discriminant*, is S_3-invariant, and is easily expressible via $a_1 = 0$, $a_2 = p$ and $a_3 = q$: $D = -4p^3 - 27q^2$. In order to describe $F(x_1, x_2, x_3)$ as a cyclic extension of $F(\sqrt{D})$, the theory instructs us to introduce Lagrange resolvents defined by the cyclic permutation σ of x_1, x_2, x_3:

$$A := x_1 + x_2 + x_3 = 0,\ B := x_1 + \zeta^{-1}x_2 + \zeta x_3,\ C := x_1 + \zeta x_2 + \zeta^{-1}x_3.$$

Here $\zeta^{\pm 1} = -(1 \mp \sqrt{-3})/2$ are the cubic roots of unity. Once A, B, C are found, the roots are easily expressed:

$$3x_1 = A + B + C,\ 3x_2 = A + \zeta B + \zeta^{-1}C,\ 3x_3 = A + \zeta^{-1}B + \zeta C.$$

On the other hand, the cubes of A, B, C are σ-invariant, and thus expressible in terms of p, q, and $\sqrt{D}$. After some computation, one obtains:

$$B^3 = -\frac{27}{2}q - \frac{27}{2}\sqrt{\frac{-D}{27}},\quad C^3 = -\frac{27}{2}q + \frac{27}{2}\sqrt{\frac{-D}{27}}.$$

In fact B and C are eigenvectors of σ with the eigenvalues ζ and ζ^{-1}, and so their product BC lies in $F(\sqrt{D})$, and even in F, since the

transposition of x_2 and x_3 interchanges B and C but preserves the product. Explicitly,

$$\begin{aligned} BC &= x_1^2 + x_2^2 + x_3^2 + (\zeta + \zeta^{-1})(x_1x_2 + x_2x_3 + x_3x_1) \\ &= (x_1 + x_2 + x_3)^2 - 3(x_1x_2 + x_2x_3 + x_3x_1) = -3p. \end{aligned}$$

From $x_1 = (B + C)/3$, we obtain *Cardano's formula*

$$x_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

where the values of the cubic roots must be chosen so that their product equals $-p/3$.

In addition to be complicated, this formula has the following peculiar property. When the coefficients p, q are real, but the discriminant $D = (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$ is negative, only one of the 3 roots is real, while the others are complex-conjugate. In this case, the formula leads to the real values of the interior square root, and when the cubic roots are interpreted as real, the sum yields the real value of x_1. However, in the case (known as the *"casus irreducibilis"*) when all 3 roots are real, so that the discriminant is positive, the interior square root spits out an imaginary value, and so the formula represents real roots via non-real numbers. Much worse than this, it requires computing a cubic root $\alpha + \beta i$ of a given complex number $a + bi$. This task, interpreted algebraically, leads to the equation $(\alpha+\beta i)^3 = a+bi$, i.e. $\alpha^3-3\alpha\beta^2 = a$, $3\alpha^2\beta - \beta^3 = b$. We can rewrite the 1st one as $4\alpha^3 - 3\alpha(\alpha^2 + \beta^2) = a$, where $\alpha^2+\beta^2 = \sqrt[3]{a^2 + b^2}$. In our case, $a = -q/2$, and $a^2+b^2 = -p^3/27$, so $\alpha^2 + \beta^2 = -p/3$. From these, we obtain the equation for α in the form $(2\alpha)^3 + p(2\alpha) + q = 0$. Thus, attempting to extract the cubic root of a complex expression in Cardano's formula, we arrive at the same cubic equation we started with!

We now turn to the quartic polynomial $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ which by substitution $x \mapsto x - a_1/4$ can be simplified into a polynomial with the zero root sum:

$$x^4 + px^2 + qx + r.$$

Its Galois group S_4 is solvable thanks to the filtration by subgroups

$$S_4 \supset A_4 \supset K_4 \supset \mathbb{Z}_2 \supset \{e\},$$

where the Klein subgroup $K_4 \cong \mathbb{Z}_2^2$ is normal, and $\mathbb{Z}_2$ stands for any of the three subgroups in K_4. The corresponding tower of field extension has the form

$$F \subset F(\sqrt{D}) \subset K \subset K' \subset E,$$

where D is the square of Vandermonde's invariant of A_4:

$$\sqrt{D} = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Note that K_4 is the kernel of the epimorphism $S_4 \to S_3$ induced by the action of S_4 on the three partitions of $\{x_1, x_2, x_3, x_4\}$ into pairs. Respectively, K is a normal extension not only over $F(\sqrt{D})$, but also over F. It is generated therefore by the following three expressions of $\{x_i\}$, invariant under K_4 but permuted arbitrarily by $S_3 = S_4/K_4$:

$$y_1 = (x_1+x_2)(x_3+x_4),\ y_2 = (x_1+x_3)(x_2+x_4),\ \ y_3 = (x_1+x_4)(x_2+x_3).$$

Consider the degree 3 polynomial with the roots y_1, y_2, y_3:

$$(y - y_1)(y - y_2)(y - y_3) = y^3 + b_1y^2 + b_2y + b_3.$$

Its coefficients b_i are S_3-symmetric functions of y_1, y_2, y_3, hence S_4-symmetric function of x_1, x_2, x_3, x_4, and can be expressed therefore via p, q, r. After some computations (taking into account that $\sum x_i = 0$), one obtains:

$$b_1 = -(y_1 + y_2 + y_3) = -2\sum_{i<j} x_ix_j = -2p, \quad b_2 = p^2 - 4r, \quad b_3 = q^2.$$

Thus, y_1, y_2, y_3 are expressible by Cardano's formulas for the cubic equation

$$y^3 - 2py^2 + (p^2 - 4r)y + q^2 = 0.$$

Now, choosing $K' = K(z)$, where $z = (x_1 + x_2)$ is invariant with respect to one of the subgroups $\mathbb{Z}_2 \subset K_4$, we find $z^2 + y_1 = 0$, since $x_3 + x_4 = -(x_1 + x_2) = -z.$ and therefore $z = \sqrt{-y_1}$.

The field K' is not normal over F. To pass from K' to E, we need therefore, following the proof of Proposition in the previous section, to adjoin the conjugate irrationalities $\sqrt{-y_2}$ and $\sqrt{-y_3}$. The values of the square roots are not independent here. Since only two quadratic extensions are needed to pass from K to E, there must be one relation between the three square roots. And indeed, the product $(x_1+x_2)(x_1+x_3)(x_1+x_4)$ is invariant under permutations of x_2, x_3, x_3, while transposing x_1 and x_2 turns it into $(x_2 + x_1)(x_2 + x_3)(x_2 + x_4)$ equal to it due to $x_1 + x_2 + x_3 + x_4 = 0$. Therefore the triple product is expressible in terms of p, q, r. And indeed,

$$\begin{aligned}(x_1 + x_2)(x_1 + x_3)(x_1 + x_4) &= \\ &= x_1^3 + (x_2 + x_3 + x_4)x_1^2 + (x_2x_3 + x_3x_4 + x_4x_2)x_1 + x_2x_3x_4 \\ &= x_1^2(x_1 + x_2 + x_3 + x_4) + \sum_{1\le i<j<k\le 4} x_ix_jx_k = -q.\end{aligned}$$

Thus, we have

$$x_1 + x_2 = \sqrt{-y_1}, \quad x_1 + x_3 = \sqrt{-y_2}, \quad x_1 + x_4 = \sqrt{-y_3}$$
$$x_3 + x_4 = -\sqrt{-y_1},\ x_2 + x_4 = -\sqrt{-y_2},\ x_2 + x_3 = -\sqrt{-y_3},$$

where the values of the square roots must be chosen so that their product $\sqrt{-y_1}\sqrt{-y_2}\sqrt{-y_3} = -q$.

Finally, the roots are computed from these as

$$x_1 = \frac{1}{2}\left(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}\right)$$
$$x_2 = \frac{1}{2}\left(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}\right)$$
$$x_3 = \frac{1}{2}\left(-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}\right)$$
$$x_4 = \frac{1}{2}\left(-\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}\right).$$

APPENDIX: AC, ZT, and ZL

A0. Formulations. A *partial ordering* "$<$" on a set P is a binary relation which is transitive, and anti-symmetric (meaning that $x < y$ and $y < x$ are impossible simultaneously). A *linear* (or *total*) ordering is a partial ordering for which any two distinct elements are comparable, i.e. $x \neq y$ implies either $x < y$ or $y < x$. A totally ordered set in which every non-empty subset has the least element is called *well-ordered*. A subset $X \subset Y$ in a totally ordered (or well-ordered) set is called an *initial segment* if for every $x \in X$ all elements of Y such that $y < x$ are also in X. A totally ordered subset of a partially ordered set is often called a *chain*. An element $x_0 \in P$ is *maximal* if P contains no $x > x_0$.

`Axiom of Choice (AC).` *The Cartesian product of non-empty sets is non-empty. Equivalently: for any set X, there is a function φ associating to every non-empty subset of X an element of this subset.*

`Zermelo's Theorem (ZT).` *Every set can be well-ordered.*

`Zorn's lemma (ZL).` *A non-empty partially ordered set, in which every chain has an upper bound, contains at least one maximal element.*

A1. ZL implies ZT. Given a set S, consider the set $\mathcal{S}$ of pairs $(X, <)$ where X is a non-empty subset of S, and $<$ is a well-ordering on X. Introduce partial ordering on $\mathcal{S}$ by $(X, <) \leq (Y, <)$ whenever $(X, <)$ is an initial segment of $(Y, <)$. Note that here $X \cup Y = Y$ is well-ordered, and the least element in X is the least in Y as well.

Let $\{(X_\alpha, <)\}$ be a chain in $\mathcal{S}$. Then $X := \cup_\alpha X_\alpha$ is well-ordered by $<$. Indeed, X is totally ordered (since any two $x_1, x_2 \in X$ belong to some X_{α_1} and X_{α_2}, whose union is well-ordered), and all X_α have the same least element. Moreover, $(X_{\alpha_1}, <)$ is an initial segment in $(X_{\alpha_1} \cup X_{\alpha_2}, <)$. Therefore $x < x_1 \in X_{\alpha_1}$ implies that $x \in X_{\alpha_1}$, and therefore $(X_{\alpha_1}, <)$ is an initial segment in $(X, <)$.

Thus, Zorn's lemma applies to $(\mathcal{S}, \leq)$, meaning that there is a maximal totally ordered subset $(S', <)$ in S. But then $S' = S$, for otherwise $x \in S - S'$ could be added to $(S', <)$ as an upper bound, contradicting its maximality.

A2. ZT implies AC. This is obvious: well-order X, and to each nonempty subset of X, associate its least element.

A3. AC implies ZL. Suppose that in a non-empty partially ordered set $(P, <)$, which does *not* have any maximal element, every chain C has an upper bound. Then the set of upper bounds not lying in C is non-empty, and using the Axiom of Choice, we can pick one for each C and denote it $\varphi(C)$.

Let $\mathcal{C}$ denote the set of *well-ordered* chains C in P such that: $\varphi(\emptyset)$ is the least element in C, and for every proper initial segment $D \subset C$, the least element in $C - D$ is $\varphi(D)$. We have: $\{\varphi(\emptyset)\} \in \mathcal{C}$.

We claim that for $C, C' \in \mathcal{C}$, one of them is an initial segment of the other. Indeed, let D be the maximal common initial segment of C and C' (i.e. the union of all common initial segments). If it is proper in both C and C', then $\varphi(D)$, being the least element in both $C - D$ and $C' - D$, can be added to D to form a larger common initial set of C and C' in conflict with the maximality of D. Thus D coincides with one of C or C' making it an initial segment of the other.

Consider now the union U of all chains from $\mathcal{C}$. As in the above derivation of Zermelo's theorem from Zorn's lemma, U is well-ordered, contains each $C \in \mathcal{C}$ as an initial segment, and has $\varphi(\emptyset)$ as its least element. We claim that $U \in \mathcal{C}$, i.e. for any proper initial segment $D \subset U$, $\varphi(D)$ is the least element in $U - D$. Indeed, an element $u \in U - D$ lies in some $C \in \mathcal{C}$, making D a proper initial segment of C, and implying that $\varphi(D)$ is the least element of $C - D$, and hence of $U - D$ as well.

By our assumption (on non-existence of maximal elements in P), U must have an upper bound not in U. But U cannot have an upper bound not in U, since in this case $U \cup \{\varphi(U)\}$ will be an element of $\mathcal{C}$ not contained in U, contradicting the choice of U. Thus, maximal elements exist.