Galois Theory

May 14, 2008

There are three flavours to this course; on the surface it appears to be a historical narrative, but as we look deeper we will see it is a survey course masquerading as a historical narrative, and finally it emerges that it is in fact a historical narrative masquerading as a survey course masquerading as a historical narrative. The course in some sense starts with the fundamental question: what are numbers? What do concepts like $\sqrt{2}$, $\sqrt[3]{2}$ and π mean, and what are the differences between the types of things these are; can we square the circle? Many of these questions were asked by the Greeks but could not be solved until much later.

The first part of the course is in many ways like high school algebra, but done properly and tying up all the loose ends. In the second part, we look at the answers to this question, and the way it leads to a rephrasing of the question itself; then, in the final part of the course we return to a narrative approach, ending in the contemporary.

Notation/Revision

Rings are taken to be commutative with multiplicative identity, e.g. $\mathbb{Z}$; a field is a ring such that $\forall r \neq 0, \exists r^{-1}$ e.g. $\mathbb{Q}, \mathbb{R}, F_p := \frac{\mathbb{Z}}{p\mathbb{Z}}$. For a ring R we denote the units in R by $R^\star$ e.g. $\mathbb{Z}^\star = \{\pm 1\}$; R is a field if and only if $R^\star = R \setminus \{0\}$. $R[x]$ is the polynomial ring in the variable x, i.e. $\{\sum_{l \geq 0} r_l x^l :$ only finitely many r_l are nonzero$\}$ considered as a ring. (We know this exists, since formally (in the same way we can construct the naturals from power sets of the empty set) $R[x]$ is the set of functions $\mathbb{N} \to R$ with finite support, with the evident ring structure; in this formalism e.g. x is the function $1 \mapsto 1, n \mapsto 0 \forall n \neq 1$, but we will not use this definition in practice). When we iterate this we write $R[x_1, \ldots, x_n]$ rather than $R[x_1] \ldots [x_n]$. If $f = \sum r_i x^i \in R[x], a \in R$ then we define $f(a) = \sum r_i a^i$, "evaluate f at a"; this gives a map $R[x] \to$ the set of functions $R \to R$. Beware; this map is neither injective nor surjective in general, e.g. $e^x \notin \mathbb{R}[x]$ for the surjectivity, and for the injectivity consider $\mathbb{Z}_p[x]$; there are only p^p functions $\mathbb{Z}_p \to \mathbb{Z}_p$ but there are infinitely many polynomials in $\mathbb{Z}_p[x]$; more explicitly x^p and x define the same function, by Fermat's little theorem.

As an exercise, the reader should show that if R has no zero divisors (i.e. is an integral domain) then $R[x]$ is an ID and $R[x]^\star = R^\star$.

If k is a field (k always denotes a field from now on) then $k[x]$ is an ED: for $a, b \in k[x], b \neq 0$ we can write $a = qb + r$ for unique q, r with $\deg r < \deg b$; this has the corollaries:

i) $k[x]$ is a PID; every ideal $I \leq k[x]$ is of the form $(f) = fk[x]$ for some $f \in I$; indeed f is an element of minimal degree in I.

ii) $k[x]$ is a UFD

iii) For $f \in k[x]$, f is irreducible iff (f) is prime iff (f) is maximal iff $\frac{k[x]}{(f)}$ is a field; this statement allows us to construct lots of fields, e.g. $\frac{\mathbb{R}[x]}{x^2+1}$.

iv) For $a, b \in k[x] \setminus \{0\}$, $(a) + (b)$ is an ideal, so a principal ideal, i.e. of the form (g), and this $g = \gcd(a, b)$.

v) If $f \in k[x] \setminus \{0\}$ then f has at most $\deg(f)$ roots in k (recall that α is a root of f means $f(\alpha) = 0$)

As an exercise the reader may proove all these; as an example, the proof of v) is done by induction on $\deg f$; if it $= 0$ f is constant and we are done; if f has no roots we are done, otherwise let α be a root, then $f(x) = (x - \alpha)g(x)$ with $\deg g = \deg f - 1$, etc.

We define $k(x)$ is the ring of rational functions on x, i.e. the fraction field of $k[x]$, the set of equivalence classes $\frac{f}{g} = \frac{r}{s}$ if $fs = rg$ over $\{\frac{f}{g} : g \neq 0\}$. Note that $k[x_1, \ldots, x_n]$ is a UFD, but not a PID if $n > 1$.

The reader should also familiarise themselves with Eisenstein's criterion, as shown on the printed sheet.

1 Algebraic and transcendental field extensions

Let L be a field and $K \subset L$ a subfield, i.e. a subring which is also a field. Unlike groups, where we would normally start from a group G and then study its subgroups $H \subset G$, when considering fields it is more profitable to start from K and then study its extensions L (we define L is an extension of K if K is a subfield of L). We write L/K for field extensions, e.g. $\mathbb{C}/\mathbb{R}, \mathbb{R}/\mathbb{Q}, \mathbb{C}/\mathbb{Q}, K(x)/K, L/K$ where $K = \mathbb{C}(z), L = \frac{\mathbb{C}(z)[y]}{y^2=z^3-z}$. We will study lots of cases of $L = \frac{K[z]}{f(z)}$ where f is irreducible as such fields appear frequently in geometry; in fact this is the function field of an elliptic curve.

We observe that if L/K is a field extension, L is a vector space over K; using this vector space structure means we can add elements of L and multiply them by elements of K; we're "forgetting" that we can also multiply elements of L and every nonzero element of L is invertible. Thus, to get a mental idea of what a field extension is, we can consider it to be a vector space with these two extra properties.

We define $[L : K]$, the degree of the field extension, as $\dim_K L$; if this is finite we say L/K is a finite extension, otherwise it is an infinite extension; e.g. $[\mathbb{C} : \mathbb{R}] = 2, [\mathbb{R} : \mathbb{Q}] = \infty$ by countability; $[\mathbb{C} : \mathbb{Q}] = \infty, [K(x) : K] = \infty$, and in our particular example above $[L : K] = 2$ by the basis $1, y$; more generally $[L : K] = \deg f$ as $1, x, \ldots, x^{d-1}$ is a basis for L.

For K a field, we always have a smallest subfield that contains 1: We always have the ring homomorphism $\mathbb{Z} \to K$ defined by $1 \mapsto 1$ (which really does define it completely), and then there are two possibilities; either this is injective in which case $\mathbb{Q} \subset K$ and we define char $K = 0$, or else $1 + \cdots + 1 = 0$ for some prime number p of 1s, in which case $F_p \subset K$ and we define char $K = p$. Then this smallest subfield is $\frac{K}{\mathbb{Q}}$ or $\frac{K}{F_p}$ respectively. For example, $F_p(x)$ has characteristic p.

We define that a field F is a finite field if $\#F$, the number of elements of F, is $< \infty$.

Lemma: let F be a finite field, then char $F = p$ for some prime p and $\#F = p^n$ for some $n \geq 1$, since $\#F < \infty \Rightarrow$ the map $\mathbb{Z} \to F$ is not injective so we must have $F_p \leq F$ for some prime p; then F is a vector space over F_p; this is necessarily finite dimensional, so $F \cong F_p^n$ as vector spaces, so $\#F = p^n$.

We shall soon see that there exists a unique finite field of order p^n for every n, but it is not unique up to unique isomorphism (the reader who understands this phrase already has nothing to learn from this course; it shall be explained in the second half of this course).

For $L/K, \alpha \in L$ define $K[\alpha]$ to be the smallest subring of L containing α and K (this notation appears as though it might be confusing, but isn't; see later); similarly $K(\alpha)$ is the smallest such field, also called the field obtained from K by adjoining α. So $K[\alpha] = \{\sum_0^n r_j \alpha^j : r_j \in K, \text{some } N\}, K(\alpha) = \{\frac{f}{g} : f, g \in K[\alpha], g \neq 0\}$. For example, $\mathbb{Q}[i] \subset \mathbb{C} = \{r_0 + r_1 i + r_2 i^2 + \ldots\} = \{r_0 + r_1 i : r_0, r_1 \in \mathbb{Q}\}$ and this is also $\mathbb{Q}(i)$.

So for x indeterminate (indeterminates will always be written x in this course) we have a ring homomorphism $\Phi : K[x] \to L$ given by $x \mapsto a$ and then $K[\alpha]$ is just the image of this Φ (so the above notational conflict isn't actually a problem). We define that α is transcendental over K if this homomorphism is injective and algebraic over K otherwise, e.g. i is algebraic over $\mathbb{Q}$ by the above.

If Φ is not injective then $\ker \Phi$ is an ideal in a PID so $= (f)$ for some f; we define the minimal polynomial of α/K ($/K$ should be read "over K) is a polynomial f of minimal degree for which $f(\alpha) = 0$; we can wlog take f monic. We define $\deg_K(\alpha)$ to be the degree of this f, e.g. $\deg_Q i = 2$ since its minimal polynomial is $x^2 + 1$. Notice that the constant in f is never zero because if it were we could divide f by x to reduce its degree; in fact we have slightly more:

Lemma: f is irreducible, as were $f = rs$ with $\deg r < \deg f, \deg s < \deg f$ then we have $f(\alpha) = r(\alpha)s(\alpha) = 0$ so one of $r(\alpha), s(\alpha)$ is 0 contradicting minimality of f.

So if α is algebraic, $K[\alpha] = \frac{K[x]}{(f)}$ with f irreducible, so $K[\alpha]$ is a field and therefore $= K(\alpha)$; note this means $K(\alpha)$ is not the image of a homomorphism $K(x) \to K(\alpha)$ if α is algebraic, since if $\phi : M \to L$ is a homomorphism of fields then it is necessarily injective.

For a direct proof that $K[\alpha]$ is a field rather than appealing to the GRM course, let $g \in K[\alpha] \backslash \{0\}$ and consider multiplication by g as a function $M_g : K[\alpha] \to K[\alpha]$ $\gamma \mapsto \gamma g$; M_g is injective as $K[\alpha] \subset L$, a field, so there are no zero divisors. M_g is a K-linear endomorphism of a finite dimensional vector space (i.e. a vector space map - the K-linear just means the vector space is over K), so since $\dim_K K[\alpha] < \infty$ it is also surjective and $\exists \gamma \in K[\alpha]$ such that $M_g(\gamma) = 1$ i.e. $g\gamma = 1$.

We have the obvious proposition that α is transcendental over $K \Leftrightarrow \Phi : K[x] \to K[\alpha]$ is an isomorphism, and hence extends to an isomorphism $K(x) \to K(\alpha)$; in particular all transcendental field extensions $K(\alpha)$ are isomorphic since they are isomorphic to $K(x)$, so e.g. $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$; we shall not study them much for this reason.

Proposition: For L/K a field extension TFAE:

i) α algebraic $/K$ ii) $[K(\alpha) : K] < \infty$ iii) $\dim_K K[\alpha] < \infty$ iv) $K[\alpha] = K(\alpha)$ v) $K[\alpha]$ is a field. These are mostly obvious other than that prooved above; for iv)$\Rightarrow$i), if $K(\alpha) = K[\alpha]$ then α^{-1} exists, call it $\sum_0^N r_i\alpha^i$ so $\sum_0^N r_i\alpha^{i+1} - 1 = 0$, an algebraic relation satisfied by α, so α is algebraic.

Warning: the notion of algebraic or transcendental depends on K e.g. $2\pi i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ with minimal polynomial $x^2 + 4\pi^2$ but transcendental over $\mathbb{Q}$ (which is a serious theorem that we may proove at the end of this course; if we do not do so then the dedicated reader is recommended to look up a proof of the result). The minimal polynomial also depends on the fiesd, e.g. for $L = \mathbb{C}, \alpha = \sqrt{i}$ the minimal polynomial is $x^4 + 1$ over $\mathbb{Q}$ but $x^2 - i$ over $\mathbb{Q}(i)$; note that the dimension of $\mathbb{Q}[\sqrt{i}]$ over $\mathbb{Q}$ is 4 while its dimension over $\mathbb{Q}[i]$ is 2 but the dimension of $\mathbb{Q}[i]$ over $\mathbb{Q}$ is also 2 and $2 \times 2 = 4$; this leads us to:

1.1 Theorem: "Tower Law"

Let $M/L/K$ field extensions: then M/K is finite iff M/L and L/K are finite, and in that case $[M : K] = [M : L][L : K]$; this follows from the more general proposition that if V is a vector space over L and L/K a finite field extension then V is finite dimensional over L iff it is finite dimensional over K and in this case $\dim_K V = \dim_L V[L : K]$; for the forward implication if x_i is a basis of V over L and l_j a basis of L over K then the $\{x_i l_j\}$ form a basis of V as a K-vector space, and if V is finite dimensional over K then it's certainly finite dimensional over L.

For example let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) \supset \mathbb{Q}$; we have from the tower law $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$ than $3 \mid [L : \mathbb{Q}]$ (as the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$) and similarly $4 \mid [L : \mathbb{Q}]$ so $12 \mid [L : \mathbb{Q}]$, but $x^4 - 5$ is a polynomial satisfied by $\sqrt[4]{5}$ over $\mathbb{Q}(\sqrt[3]{2})$, so $[L : \mathbb{Q}(\sqrt[3]{2})] \leq 4$ and $[L : \mathbb{Q}] \leq 12 \therefore = 12$; therefore $[L : \mathbb{Q}(\sqrt[3]{2})] = 4$ so $x^4 - 5$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$ (which is unsurprising).

For example, let $\omega = e^{\frac{2\pi i}{p}}$ where p is an odd prime, $\alpha = \omega + \omega^{-1}$; what is $\deg_{\mathbb{Q}} \alpha$? We have $\omega^p = 1$ so ω is a root of $\frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1} = f(x)$; this is irreducible over $\mathbb{Q}$ by eisenstein's criterion on $f(x + 1)$; the reader is once again advised to familiarise themselves with this.

So $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$; now $\alpha \in \mathbb{Q}(\omega)$ so by the tower law on $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\omega)$, $\deg_{\mathbb{Q}}(\alpha) \mid p - 1$, but $\omega^2 - \alpha\omega + 1 = 0$ so ω is a root of $x^2 - \alpha x + 1$ over $\mathbb{Q}(\alpha)$; $\mathbb{Q}(\alpha) \subset \mathbb{R}$ but $\mathbb{Q}(\omega)$ not so $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)] > 1$ so it must $= 2$ and so by the tower law $]\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{p-1}{2}$.

1.2 Corollaries of the tower law

If L/K is a finite extension and $\alpha \in L$ then α is algebraic over K and $\deg(\alpha) \mid [L : K]$, since $K \subset K(\alpha) \subset L$; therefore if $[L : K] = p$ prime and $\alpha \in L \setminus K$ then $K(\alpha) = L$ as $[K(\alpha) : L] \mid p$ and $\neq 1$.

$\alpha_1, \ldots, \alpha_n$ are algebraic over K iff $[K(\alpha_1, \ldots, \alpha_n) : K] < \infty$: for the reverse implication if $K(\alpha_1, \ldots, \alpha_n)$ is finite over K then $K(\alpha_i$ is a subspace therof so also finite over K, for the forward implication we induct; α_{i+1} is algebraic over K so algebraic over $K(\alpha_1, \ldots, \alpha_i)$ (since it satisfies the same polynomial it does over K), so by tower law on $K(\alpha_1, \ldots, \alpha_{i+1})/K(\alpha_1, \ldots, \alpha_i)/K$, $K(\alpha_1, \ldots, \alpha_i)$ is finite.

As a particular case of this, if α, β are algebraic then so are $\alpha + \beta, \alpha\beta, \frac{\alpha}{\beta}$ (for $\beta \neq 0$); we can find the polynomials they satisfy explicitly by, if we e.g. want to find $\gamma = \alpha + \beta$, considering $1, \gamma, \gamma^2$ etc, using our algebraic relations for α, β

to simplify these, and looking for a linear relation. (Excercise: if a, b, ab are not squares then $[K(\sqrt{a} + \sqrt{b}) : K] = 4$.

Corollary: if L/K is a field extension then the elements of L which are algebraic over K form a subfield.

We define an extension L/K is algebraic if every $\alpha \in L$ is algebraic over K; for example, a finite extension L/K, $K(\alpha)$ for α algebraic, or $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ algebraic } /\mathbb{Q}\}$; this is a field and by definition each of its elements is algebraic. Note that $\dim \overline{\mathbb{Q}} = \infty$ as e.g. $\sqrt[n]{3} \in \overline{\mathbb{Q}} \forall n$ and $[\mathbb{Q}(\sqrt[n]{3}) : \mathbb{Q}] = n$ so $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n \forall n$.

As an aside, an extension L/K is algebraic iff L is the (possibly infinite) union of its subfields which are finite over K.

Lemma: for $M/L/K$ field extensions, M/K is algebraic iff M/L and L/K are; for the forward implication if M/K algebraic then $\alpha \in M$ is algebraic over K so certainly algebraic over L, and $L \subset M$ must be algebraic over K; for the reverse if $\alpha \in M$ algebraic over L then $r_0 + r_1\alpha + \cdots + r_d\alpha^d = 0$ for some $r_0, \ldots, r_d \in L$; set $L_0 = K(r_0, \ldots, r_d)$; then each r_i is algebraic over K (as L is algebraic over K) so L_0 is finite over K; α is algebraic over L_0 so $[L_0(\alpha) : L_0] < \infty$ and by the tower law $[L_0(\alpha) : K] < \infty$ so α is algebraic over K.

1.5: Interlude: Constructions with Ruler and Compass

This section is non-examinable. The probably-innacurate history is that a few thousand years ago the Greeks were trying to understand the real numbers. They had discovered that $\sqrt{2}$ is irrational, but now what is $\sqrt[3]{2}$? Clearly it is irrational, but is it "worse" than $\sqrt{2}$? In actuality the Greeks had discovered almost all of the content of this section - they knew how to approximate cubics arbitrarily closely (at least as applied to geometric problems), or solve the three classical problems we will mention here with the use of conic sections and other curves - they just didn't have the "right formalism" to express their solutions, i.e. algebra.

We will show that certain geometrical constructions are impossible with "straightedge and compass". More formally, we call some points "constructible"; the set of constructible points is defined inductively as follows:

We are initially given two constructible points

The line through two constructible points is called a constructible line

The intersection point of two constructible lines [if it exists] is constructible

The circle with center a constructible point passing through another constructible point is called a constructible circle [private definition].

If they/it exists, the intersection points of a constrictible line and a constructible circle, or of two constructible circles, is constructible.

There is something of a "game" of discovering which points are constructible, and it is important to appreciate how much of an achievement many of these results were for the Greeks, who hadn't grown p with algebra the way we do. However, we will now solve this game.

First, some examples of what we can do:

1) We can draw the line through a constructed point P perpendicular to the constructed line QR: for P on QR, firstly we draw the circle (P,Q) (i.e. the circle with centre P through Q) and let Q' be its intersection with QR (not at Q); then we draw the circle (Q, Q') and the circle (Q', Q). The line through the two points where these two circles intersect is then the required line. For P not on QR, we

draw the circle (P,Q), and call the intersection of this with QR Q', then proceed as before.

2) We can draw the line parellel to a line l passing through a point P; we draw the line k through P perpendicular to l by 1), then the line through P perpendicular to k, again by 1).

3) We can mark off a length defined by two constructible points Q,R on another line l, starting from a point P on l: construct the line parallel to l through R, draw the circle (R,Q) to obtain the point Q' in the "right" direction, [then draw the line parallel through RP through Q' and its intersection with l is the required point].

These examples imply we can construct cartesian coordinates in the plane - we make the initial points be $(0, 0)$ and (0,1).

Definition: $\lambda \in \mathbb{R}$ is constructible if $|\lambda|$ is the distance between two constructible points.

Lemma: p=(a,b) is constructible $\Leftrightarrow$ $(a, b) \in \mathbb{R}$ is constructible: for the forward implication, given p we can take its coordinates by dropping perpendiculars to the x and y axes, for the reverse mark off the distances along the x and y axis, construct perpendiculars to the axes at these, and their intersection is p.

Proposition: the constructible real numbers form a subfield of $\mathbb{R}$, isnce if a, b are constructible so are $a + b, -a, ab$ and $\frac{1}{a}$ (for $a \neq 0$; the first two are obvious from example 3) above, for multiplication and division we use similar triangles; given a right triangle of line segments r, s and hypotenuse l_1, and another line segment r' from the same line as r, we can construct a similar triangle by drawing $l_2 \parallel l_1$ and $s' \perp r'$ to meet it. Then we have $\frac{r}{s} = \frac{r'}{s'}$, so we can construct $s' = ab$ by setting $r = 1, s = a, r' = b$ and $s' = \frac{1}{a}$ by $r = a, s = 1, r' = 1$.

Proposition: if $a > 0$ is constructible so is $\sqrt{a}$; draw the circle of diameter $a+1$; then construct the line y perpendicular to a diameter l of the circle through a point p on l, 1 away from the circumference. Then draw the radius to the intersection of y and we have a right angled triangle of base $\frac{a-1}{2}$ and hypotenuse $r = a + 1$ so by pythagoras $y = \sqrt{a}$.

Theorem: let $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n = K \subset \mathbb{R}$ be a chain of subfields of $\mathbb{R}$ such that ($\star\star$) for each i, F_{i+1} is obtained by adjoining $\sqrt{r}$ to F_i where $r \neq 0 \in F_i$ and r is not a square in F_i. Then every element of of K is a constructible real number, and if $a \in \mathbb{R}$ is constructible then there is such a chain of subfields with $a \in K$: for the forward implication every element of K is constructible by the previous propositions. For the converse, an exercise, we set $F_0 = \mathbb{Q}$ and induct on the number of steps needed to construct a (recall we start with $(0, 0), (1, 0)$; the intersection of lines constructed through points in F_i is still in F_i, and intersection of two circles or a circle and a line can only introduce square roots.

Corollary: If $a \in \mathbb{R}$ is constructible then it is algebraic over $\mathbb{Q}$ with $\deg_{\mathbb{Q}} a = 2^i$ for some i; the proof is immediate by the tower law. Note the converse is false; not all reals of degree 2^i over $\mathbb{Q}$ are constructible.

Now we move on to solve three great problems of antiquity; first, "squaring the circle", constructing a square whose area is the same as that of a circle of radius 1, is impossible as it necessitates constructing $\sqrt{\pi}$ which is impossible since π is transcendental (but this is not a "real" solution as we have yet to actually proove the transcendentality of π. Second, "duplicating the cube", constructing a cube whose volume is twice that of a given cube, requires constructing $\sqrt[3]{2}$

but the degree of this over $\mathbb{Q}$ is 3 so it is impossible. Finally, we cannot trisect angles in general; it suffices to proove that we cannot trisect $\frac{\pi}{3}$; $\cos\frac{\pi}{3} = \frac{1}{2}$ so it is constructible, but $\cos\frac{\pi}{9}$ ain't; let $\alpha = \cos\frac{\pi}{9}$ and we will show this is algebraic but of degree 3; for any θ, $\cos 3\theta = 4\cos^3\theta = 3\cos\theta$ (as $(e^{i\theta})^3 = \cos 3\theta + i\sin\theta$ etc.); putting $\theta = \alpha$ we get $\frac{1}{2} = 4\alpha^3 - 3\alpha$ i.e. α is a root of $8x^3 - 6x - 1$, but this is irreducible over $\mathbb{Q}$ (to proove this, we just need to check that there are no linear factors $ax + b$; we can do this using Gauss' lemma to find that we would need $b = \pm 1, a = 8$ and check cases, or by eisenstein, or by checking all the possible values modulo 5). Finally, the regular p-gon for p prime is not constructible if $p - 1$ is not a power of 2, since this amounts to constructing $\cos\frac{2\pi}{p}$, but we showed last lecture that this has degree $\frac{p-1}{2}$ (since it is $\frac{1}{2}(e^{\frac{2\pi i}{p}} + e^{-\frac{2\pi i}{p}})$). For which numbers are constructible in general, see later; Gauss showed which n-gons can be constructed, but this leads into polynomials, and thence into quintics and the "big result" of this course.

2 Splitting Fields

Let $f \in K[X]$ Then a field extension L/K is a splitting field for f if $f = (x - \alpha_1)\ldots(x - \alpha_d)$ in L (i.e. f splits into linear factors) and $L = K(\alpha_1, a\ldots, \alpha_d)$ where the α_i are the roots of f in L. Examples are for $K = \mathbb{Q}$, $\mathbb{Q}(i)$ is a splitting field for $f(x) = x^2 + 1$ over Q, and $\mathbb{Q}(\alpha, \alpha\omega)$ is a splitting field for $f(x) = x^3 - 2$ over $\mathbb{Q}$ where α is the (real) cube root of 2 and $\omega = e^{\frac{2i\pi}{3}}$. Note that $\deg_{\mathbb{Q}}\alpha = 3 = \deg_{\mathbb{Q}}(\alpha\omega) = \deg_{\mathbb{Q}}(\alpha\omega^2)$ (and these are the three roots of f), as each of these has minimal polynomial $x^3 - 2$. However, $\deg_{\mathbb{Q}}\omega = 2$ since $\frac{x^3-1}{x-1}$ is its minimal polynomial, so we have $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 > 3$; notice that this field is obtained by adjoining two of the roots of f, one is insufficient. A final example is that for $f(x) = \frac{x^p-1}{x-1}$ with p prime (this is $\prod_1^{p-1}(x - \omega^i)$ where $\omega = e^{\frac{2\pi i}{p}}$, $\mathbb{Q}(\omega)$ is a splitting field, of degree $p - 1$.

The existence of splitting fields is not as obvious as it might seem. In the above examples we had $\mathbb{C}$ as a containing field, so we knew that the roots of the polynomials existed (since we could factorize them over $\mathbb{C}$, and could obtain the splitting fields by just adjoining all these roots from $\mathbb{C}$. However, in general, we have no such containing field; given an arbitrary field K it is not at all clear that we can extend this to a field in which a given polynomial can be factored. However, we have the following:

Theorem: existence of splitting fields: for any $f \in K[x]$, a splitting field for f over K exists. If f is irreducible then $\frac{K[x]}{(f)}$ is a field, called K_f. Then K_f/K is a field extension; put $\alpha = x + (f) \in K_f$. It is then clear that $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ where $d = \deg f = \deg_K(\alpha)$ forms a basis for K_f/K and $f(\alpha) = f(x) + (f) = (f) = 0$ in K_f. So $K_f = K(\alpha)$ where $f(\alpha) = 0$; this is the field obtained from K by adjoining one root α of f. Now we just iterate this to proove the theorem: we induct on $\deg f$; if $\deg f = 1$ then $K_f = K$ and we are done, otherwise we assume that any polinomial of degree $< \deg f$ over any field K has a splitting field, then let g be an irreducible factor of f and consider $K_g = \frac{K[t]}{(g)}$; let $\alpha = t + (g)$, then $g(\alpha) = 0$ in K_g, so since $g \mid f$, $f(\alpha) = 0$ so $f(x) = (x - \alpha)f_1(x)$ for some $f_1(x) \in K_g[x]$. Now by the inductive hypothesis there is a splitting field $L = K_g(\alpha_2, \ldots, \alpha_d)$ for f_1 over K_g where $\alpha_2, \ldots, \alpha_d$ are the roots of f in L. Then L is a splitting field for f over

K, since f factors as $f(x) = (x - \alpha)f_1(x) = (x - \alpha)(x - \alpha_2)\dots(x - \alpha_d)$ and since $K_g = K(\alpha)$, $L = K(\alpha)(\alpha_2, \dots, \alpha_d)$ as required.

2.1 Uniqueness of splitting fields

This is quite subtle, and in a sense the heart of the course: for example, consider $K = \mathbb{R}$ and we want to construct $\mathbb{C}$. The obvious way to do this is to set $f(x) = x^2 + 1$ and define $\mathbb{C} = \mathbb{R}_f = \frac{\mathbb{R}[x]}{x^2+1}$; this builds $\mathbb{C}$ with a distinguished element i, the image of x in $\frac{\mathbb{R}[x]}{x^2+1}$. Now suppose we instead took $g(y) = y^2 + 2y + 2$ (i.e. $(y + 1 + i)(p + 1 - i)$), and consider $\frac{\mathbb{R}[y]}{y^2+2y+2} = \mathbb{R}_y$; this is also isomorphic to $\mathbb{C}$, and has a distinguished element, the image of y. But there is no canonical way to identify this with either $-1 - i$ or $-1 + i$; we have two equally valid isomorphisms $\mathbb{R}_g \to \mathbb{R}_f$ given by $y \mapsto -1-x, y \mapsto -1+x$, but we have to choose which we use.

Theorem: "uniqueness of splitting fields". Let $f \in K[x], L$ a splitting field for f. If $\phi : K \hookrightarrow M$ [This curly arrow denotes injectivity; recall field homomorphisms are always injective] is a homomorphism of fields and $\phi(f)$ splits (into linear factors) in M, $f(x) = \sum a_i x^i, \phi(f) = \sum \phi(a_i)x^i \in M[x]$, then we can extend ϕ to a homomorphism $\bar{\phi} : L \to M$, and moreover firstly if M is a splitting field for f then $\bar{\phi}$ is an isomorphism, and secondly the number of such homomorphisms $\bar{\phi}$ is $\leq [L : K]$ with equality iff f has no multiple roots in L (and hence in M): we induct on $[L : K]$. If f splits in K i.e. $[L : K] = 1$ then we are done, otherwise let $\alpha_i \in L \setminus K$ be a root of f, and g the minimal polynomial of α_1 over K. Now, we will use the following key lemma, which we shall proove in a moment: for L/K a field extension and $g \in K[x]$ an irreducible polynomial, there is a bijection between homomorphisms $\tilde{\phi} : K_g \to L$ such that $\tilde{\phi}(k) = k \forall k \in K$ and roots α of g in L. By this, homomorphisims $K(\alpha_1) \to M$ biject with roots of $\tilde{\phi}(g)$ in M. As $\phi(f)$ splits in M and $g \mid f$, $\phi(g)$ splits in M, so there are $\leq \deg g = [K(\alpha_1) : K]$ homomorphisms with equality iff g has distinct roots. Now we induct by applying the result with K replaced with $K(\alpha)$; choose a homomorphisim $\phi' : K(\alpha) \to M$ extending ϕ (this is equivalent to choice of a root of g); $[L : K(\alpha)] < 0L : K]$ so we may induct; $\bar{\phi}$ exists and the number of such extensions is $\leq [L : K(\alpha)]$, so the total number of homomorphisms is $\leq [L : K(\alpha)][K(\alpha) : K] = [L : K]$ with equality if there are repeated roots.

Now, for the first property, if M is a splitting field then $M = K(\beta_1, \dots, \beta_d)$ where β_i are the roots of f (or strictly $\phi(f)$), but if $\bar{\phi} : L \to M$ is a homomorphism and α_i are the roots of f in L then $\bar{\phi}(\alpha_i)$ are roots of f in M, so the image of $\bar{\phi}$ contains all the β_i, so $\bar{\phi}$ is surjective; it is automatically injective.

Define that if $L/K, M/K$ are extensions of K then a homomorphism $\phi : L \to M$ is a K-homomorphism if $\phi\mid_K = id$, i.e. $\phi(k) = k \forall k \in K$, e.g. $z \mapsto \bar{z}$ is an $\mathbb{R}$-homomorphism but not a $\mathbb{C}$-homomorphism.

Now, a proof of the key lemma from above: for L/K a field extension and $f \in K[x]$ there is a bijection between K-homomorphisms $\phi : K_f \to L$ and roots α of f in L, where K_f is the field $\frac{K[x]}{(f)}$: a K-homomorphism $\frac{K[x]}{(f)} \to L$ is precisely a ring homomorphism $\phi : K[x] \to L$ such that firstly $\phi(k) = k \forall k \in K$ and secondly $\ker\phi = (f)$, by the first isomorphism theorem. Such a ϕ is determined by $\phi(x)$, since then we have $\phi(\sum r_i x^i) = \sum \phi(r_1)\phi(x)^i$. But $\phi(f(x)) = f(\phi(x))$, so $\phi(f) = 0 \Leftrightarrow \ker\phi \supset (f)$; since f is irreducible the ideal generated by f is maximal so this $\Leftrightarrow \ker\phi = (f) \Leftrightarrow \phi(x)$ is a root of f in L. Note that this implies the number of K-homomorphisms $K_f \to L$ is finite and $\leq \deg f$.

Corollary: If $\alpha, \beta \in L$ are algebraic over K, then $\exists$ a K-isomorphism $K(\alpha) \to K(\beta)$ with $\alpha \mapsto \beta \Leftrightarrow \alpha, \beta$ have the same minimal polynomial; for the reverse implication if f is the minimal polynomial for both α and β then we have isomorphisms $K_f \to K(\alpha), K(\beta)$; for the forward implication, if there is a K-isomorphism $\theta : K(\alpha) \to K(\beta)$ then we have an isomorphism $K_f \to K(\beta)$ where f is the minimal polynomial of α, so by the key lemma $f(\beta) = 0$ and the minimal polynomial g of β divides f, but similarly $f \mid g$ so $f = g$.

Example: For $K = \mathbb{Q} \subset \mathbb{C}, f(x) = x^3 - 2$ with roots $\alpha, \alpha\omega, \alpha\omega^2$ with $\alpha \in \mathbb{R}$ as before. Since both $\alpha, \alpha\omega$ have minimal polynomial f there is a $\mathbb{Q}$-isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha\omega)$. Note that $\mathbb{Q}(\alpha) \subset \mathbb{R}$ but $\mathbb{Q}(\alpha\omega)$ is not a subset of $\mathbb{R}$; this isomorphism "sees only the internal structure of the field", not how the fields "sit" in $\mathbb{C}$.

3 Finite Fields and Separability

Which fields do we know exist? Thus far we only really know about $\mathbb{Q}$ (which we constructed from $\mathbb{Z}$), $\mathbb{R}$ which was a closure of $\mathbb{Q}$, $\mathbb{C}$ an extension of $\mathbb{R}$, and the finite fields $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (if the reader has seen the p-adics we will know about these as well). In this section we shall construct all the finite fields.

Proposition: For K a field and $G \leq K^\times$ a <u>finite</u> subgroup, G is cyclic: G is abelian so by the structure theorem for finite abelian groups $G \cong \frac{\mathbb{Z}}{m_1} \times \cdots \times \frac{\mathbb{Z}}{m_r}$ where $m_1 \mid m_2 \mid \cdots \mid m_r$ and $\#G = m_1 \dots m_r$. So if $\alpha \in G$ then $\alpha^{m_r} = 1$, since each $m_i \mid m_r$, i.e. every element of G is a rooot of $x^{m_r} - 1$. But there are at most m_r such roots, so we have $m_1 m_2 \dots m_r \leq m_r$, so $r = 1$ i.e. $G = \frac{\mathbb{Z}}{m_r}$ and G is cyclic.

Corollary: if $\#K$ is finte then $K^\times$ is a cyclic group, of order $p^n - 1$ (since we already have $\#K = p^n$, e.g. $F_7^\times = \langle 3 \rangle$. However, this is nonconstructive - there is no way of guessing a generator, and e.g. 2 does not generate $F_7^\times$; in fact there is no canonical choice of generator even in F_p.

Let K be a finite field, $\#K = q = p^n$ with p prime. Then every $\alpha \in K$ satisfies $\alpha^q = \alpha$, i.e. is a root of $x^q - x$, and $x^q - x = x(x^{q-1} - 1)$ factors into linear factors with distinct roots, since any $\alpha \neq 0$ is a root of $x^{q-1} - 1$ and there are $q - 1$ distinct such α; $\alpha = 0$ is a root of x, so K is a splitting field of $x^q - x$ over F_p. We now have uniquemess given the order $\#K = q = p^n$; we want to show such a K always exists, but we can do this by defining it as the splitting field of $x^q - x$ over F_p, so now we just need to prove that $x^q - x$ has distinct roots, and the splitting field so defined will have size q as required:

For K a field, define the formal derivative $\frac{d}{dx}|K[x] \to K[x]$. This is a K-linear map defined by $x^n \mapsto nx^{n-1}$; the reader may verify as an exercise the "Leibnitz rule" that $\frac{d}{dx}(fg) = \frac{df}{dx}g + f\frac{dg}{dx}$ and the chain rule $\frac{d}{dx}f(g(x)) = \frac{df}{dx}(g(x))\frac{dg}{dx}$. We write $f'(x)$ for $\frac{df}{dx}$ where this would not be ambiguous. Note that this is "not a trick"; the ability to do calculus in these fields is enormously useful and widely applicable.

Lemma: For L/K a field extension, $\alpha \in L, f \in K[x]$, α is a simple root (i.e. occurs only once) iff $f'(\alpha) \neq 0$: $f(x) = (x - \alpha)g(x)$ by Leibnitz $\Rightarrow f'(x) = (x - \alpha)g'(x) - g(x)$, so this is 0 iff $g(\alpha) = 0$ i.e. f has multiple roots iff $\gcd(f, f')$ has degree > 1.

Example: Let K be a field of characteristic p and $k \in K$ not a pth power, e.g. $K = F_p(y)$ the field of rational functions in $y, b = y$. Consider $f(x) = x^p - b \in K[x]$; let L be a splitting field for f over K, $\alpha \in L$ a root of f, i.e. $\alpha^p = b$. Then $f'(x) = px^{p-1} = 0 \Rightarrow \alpha$ is a multiple root; in fact $(x - \alpha)^2 = x^p - \binom{p}{1}x^{p-1}\alpha + \cdots + (-\alpha)^p = x^p + (-\alpha)^p = x^p - \alpha^p$ (since if p is even, i.e. 2, then + is the same as -).

We shall now abandon this example.

Proposition: For R a ring, char $R = p$, the map $F : R \to R$ $x \mapsto x^p$ is a ring homomorphism, called the "Frobenius" map: we just need that $F(x + y) = Fx + Fy$, i.e. $(x + y)^p = x^p + y^p$, but $(x + y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + y^p$, and $p \mid \binom{p}{i} \forall 0 < i < p$.

Theorem: finite fields exist and are unique: let $q = p^n, n \geq 1, p$ prime, then 1) there is a field F_q with $\#F = q$, and any field of q elements is isomorphic to this, 2) F_q is the splitting field of $x^q - x$ over F_p, and 3) F_q contains a subfield of order p^k iff $k \mid n$. Clearly $2 \Rightarrow 1$, as above; for 2), let K be the splitting field of $x^q - x$ over F_p, so $K = F_p(\alpha_1, \ldots, \alpha_q)$ where $\alpha_i^q = \alpha_i$. If α, β are two roots of $x^q - x$ then so are $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ for $\beta \neq 0$; the last two of these are obvious, and $(\alpha + \beta)^{p^n} = (\alpha^p + \beta^p)^{p^{n-1}} = \cdots = \alpha^{p^n} + \beta^{p^n}$ by repeated application of Frobenius. Therefore the field generated by the roots of $x^q + x$ is just the union of the roots, so $\#K \leq q$. But if α is a root of $x^q - x$ then it is not a root of $\frac{d}{dx}(x^q - x) = -1$, so $x^q - x$ has q distinct roots and $\#K = q$. For 3), for the only if part, if $F_p \subset L \subset F_q$ then $\#L = p^l$ for some l, then by the tower law $l \mid n$; for the if part is sufficient to prove that $x^{p^l} - x \mid x^{p^n} - x$ if $l \mid n$, since then $\{\alpha \in F_q : \alpha^{p^l} = \alpha\}$ is a subfield as required by 2). But $y - 1 \mid y^s - 1 = (y - 1)(1 + y + \cdots + y^{s-1})$, so applying this with $y = x^r$, $x^r - 1 \mid x^{rs} - 1$; then applying this with $r = p^l - 1, rs = p^n - 1, n = lk$ say; we have $p^l - 1 \mid p^{lk} - 1$.

Note that $F_q \neq \frac{\mathbb{Z}}{q\mathbb{Z}}$, in general.

3.5: Separability

Define $f \in K[x]$ is separable if it splits into distinct linear factors in a splitting field; otherwise it is inseparable. For example, $X^q - X \in F_p[X]$ is separable, but $x^p - y \in F_p(y)[x]$ is inseparable. So f is separable iff $\gcd(f, f') = 1$.

Proposition: 1) Let $f \in K[x]$ be irreducible, then f is separable iff $f' \neq 0$ 2) If char $K = 0$ then every irreducible polynomial is separable 3) If char $K = p$ then an irreducible $f \in K[x]$ is inseparable iff $f(x) = g(x^p)$ for some $g \in K[x]$. For 1), wlog take f monic; f is irreducible so $\gcd(f, f')$ must be 1 or f; if $f' = 0$ then this gcd is f, i.e. f has multiple roots so it is inseparable, otherwise as $\deg f' < \deg f$ this gcd cannot be f so it must be 1 and f is separable. For 2) and 3), if $f(X) = \sum r_i X^i$ then $f'(X) = \sum_{i \geq 1} i r_i X^{i-1}$ so $f'(X) = 0 \Leftrightarrow i r_i = 0 \forall i \geq 1$; if char $K = 0$ then $i r_i = 0 \Rightarrow r_i = 0$, so f is a constant (which by convention we take to not be irreducible); if char $k = p$ then $i r_i = 0 \Rightarrow r_i = 0$ whenever $p \nmid i$, so $f(X) = \sum_{i \geq 0} r_{pi} X^i = g(x^p)$ for $g(x) = \sum r_{pi} x_i$.

Definition: 1) If α is algebraic over K then α is separable iff the minimal polynomial of α is; otherwise it is inseparable. 2) An extension L/K is separable iff every $\alpha \in L$ is separable over K; for example if char $K = 0$ then all algebraic extensions are separable; we shall see later that separable extensions are the "correct" analogue of algebraic extensions in fields of other characteristics. If char $K = p$, $F_p(y^{\frac{1}{p}})$ is inseparable.

Corollary of key lemma: let α be algebraic over K with minimal polynomial f and L/K be an extension in which f splits, then α is separable iff there are exactly $\deg f = \deg \alpha$ K-homomorphisms $K(\alpha) \to L$.

Proposition: Suppose α algebraic and separable over K, then $\frac{K(\alpha)}{K}$ is separable, i.e. all $\beta \in K(\alpha)$ are separable. The proof is by counting; let f be the minimal polynomial of α over K, $\beta \in K(\alpha)$, g the minimal polynomial of β over K, with $m = \deg g$. Let M be a splitting field for fg; this means in particular that M is an extension in which g splits, so by the key lemma we need to show that there are precisely $m = \deg g$ K-homomorphisms $K(\beta) \to M$, then β is separable and we are done. Map from the set of K-homomorphisms $\phi : K(\alpha) \to M$ to the set of K-homomorphisms $\bar{\phi} : K(\beta) \to M$ by $\phi \mapsto \bar{\phi} := \phi \mid_{K(\beta)}$; since α is separable there are $[K(\alpha) : K] = mn$ such ϕ by the key lemma; we have that there are $\leq [K(\beta) : K]$ such $\bar{\phi}$ and need to show equality. Since α is separable over K it is separable over $K(\beta)$, since roots of its minimal polynomial remain distinct as its minimal polynomial over $K(\beta)$ divides its minimal polynomial over K. So for a given $\bar{\phi} : K(\beta) \to M$ there are precisely $n = [K(\alpha) : K(\beta)]$ $K(\beta)$-homomorphisms $\phi : K(\alpha) \to M$ extending $\bar{\phi}$ (by the key lemma), so the fibres (definition: if $f : X \to Y$ is a map then $f^{-1}(y) = \{x \in X : f(x) = y\}$ is called the "fibre of f" (at y); the term comes from projection maps, since if we are e.g. projecting a 3D surface onto a 2D plane, this set really does look like a fibre) of the map $\phi \mapsto \bar{\phi}$ have cardinality exactly n, so the number of distinct $\bar{\phi}$ is $\frac{mn}{n} = m$ as required.

We will often use this trivial proposition: i) for L/K a field extension, $f, g \in K[x]$, $\gcd(f,g)$ is the same whether computed in $K[x]$ or $L[x]$; hence $\mathrm{lcm}(f,g) = \frac{fg}{\gcd(f,g)}$ is also: put $h = \gcd_K(f,g), h_1 = \gcd_L(f,g)$, then $h \mid f, h \mid g$ in $K[x]$ so also in $L[x]$ so $h \mid h_1$ is $L[x]$, but $h = pf + qg$ for some $p, q \in K[x]$ so $h_1 \mid h$ in $L[x]$ so $(h) = (h_1)$, and ii) the lcm of a finite set of separable polynomials is separable, since we can compute the lcm in any field extension; choose one in which all the polynomials split into linear factors, which are distinct (within each polynomial) by hypothesis, then the lcm clearly also splits into distinct linear factors.

The following theorem is very important, much more so than its immediate application that M/K is separable if $M/L, L/K$ are. In some sense it is the first real theorem of the course.

Theorem of the primitive element: let $L = K(\alpha_1, \ldots, \alpha_n, \beta)$, L/K a finite extension [implying β is algebraic], each α_i separable over K. Then $\exists \gamma \in L$ such that $L = K(\gamma)$ - this result is new even in characteristic 0 where all algebraic things are separable. If $\#K < \infty$ then $\#L < \infty$ so $L^\times$ is a cyclic group; let γ be a generator therof, then $L = K(\gamma)$. Otherwise, $\#K = \infty$: we induct on n; if we can show $K(\alpha, \beta)$ is $K(\gamma)$ with γ separable, then $K(\alpha_1, \beta) = K(\beta_1$ for some β_1 so $K(\alpha_1, \alpha_2, \beta) = K(\alpha_2, \beta_1) = K(\beta_2)$ for some β_2, etc. We will show that for "most" [i.e. almost all] $c \in K$ the subfield $K(\beta + c\alpha)$ is L; then we can put $\gamma = \beta + c\alpha$ and we are done. We will do this by determining the minimal polynomial of α over $K(\gamma)$; we need that it has degree 1.

Let f be the minimal polynomial of α/K (this notation is read "over K"), g the minimal polynomial of β/K, M a splitting field for fg. In M, $f(x) = (x - \alpha)(x - \alpha'_2)\ldots(x - \alpha'_n)$ with α and all the α'_i distinct since α is separable; $g(x) = (x - \beta_1)\ldots(x - \beta_m)$. Consider $h(X) = g(\gamma - cX) \in K(\gamma)[X]$; $h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0, f(\alpha) = 0$ so $x - \alpha \mid \gcd(f, h)$. If f and h have no other common roots, we win, since then $\gcd(f, h) = X - \alpha \therefore X - \alpha = fp + hq$ for some polynomials

$p, q \in K(\gamma)[X]$ so $X - \alpha \in K(\gamma)[X]$. To compute $\gcd_{K(\gamma)}(f, h)$ we only need to compute $\gcd_M(f, h)$, so it is enough to show $h(\alpha'_i) \neq 0 \forall 2 \leq i \leq n$. But $h(\theta) = 0 \Leftrightarrow g(\gamma - c\theta) = 0 \Leftrightarrow \gamma - c\theta = \beta_j$ for some j. But $\gamma = \beta + c\alpha$ so $h(\alpha'_i) = 0 \Leftrightarrow \exists j : \beta_j - \beta = c(\alpha - \alpha'_i)$, so $h(\alpha'_i) = 0$ only for $c \in \{\frac{\beta_j - \beta}{\alpha - \alpha'_i}\}$, a finite set; as $\#K = \infty$ we can choose a c for which this is not the case.

An example: $K = \mathbb{Q}, L = \mathbb{Q}[\sqrt[3]{2}, i]$; $[L : K] = 6$. $\beta_1 = i, \beta_2 = -i, \alpha = \sqrt[3]{2}, \alpha'_2 = \omega\alpha, \alpha'_3 = \omega^{-1}\alpha$ where $\omega = e^{\frac{2\pi i}{3}}$; note $M \supsetneq L$. So $L = \mathbb{Q}[i + c\sqrt[3]{2}]$ for any $c \neq 0 \in \mathbb{Q}$, since the set we have to avoid here is $\frac{\pm i - i}{\sqrt[3]{2}(\omega^{\pm 1} - 1}$, which does not intersect $\mathbb{Q}$.

An exercise, to contemplate rather than actually do: $1, \sqrt[3]{2}, (\sqrt[3]{2})^2, i, i\sqrt[3]{2}, i(\sqrt[3]{2})^2$ form a basis of $L/\mathbb{Q}$ so an arbitrary element $\gamma \in L$ is a linear combination of these. For each such γ, determine the subfield $K(\gamma) \subset \mathbb{Q}(i, \sqrt[3]{2})$; in particular, show there are only finitely many subfields.

Corollary: If $\frac{L}{K}$ is finite and separable then $L = K(\gamma)$ for some $\gamma \in L$.

Proposition: For $M/L, L/K$ finite separable extensions, M/K is finite separable: $L = K(\alpha), M = L(\beta)$ by the theorem of the primitive element, so $M = K(\alpha, \beta)$; by the theorem of the primitive element $M = K(\gamma)$ some γ, so we now just need to show γ is separable over K. We have $K \subset K(\alpha) \subset K(\alpha, \beta) = K(\gamma)$; let $m = [K(\alpha), K], n = [K(\gamma) : K(\alpha)]$, then $[K(\gamma) : K] = mn$. Let T de a field in which the minimal polynomials of α, β, γ split, then for γ separable we need to show there are mn K-homomorphisms $K(\gamma) \to T$: since α separable $/K$ there are m distinct K-homomorphisms $K(\alpha) \to T$, but β is also separable $/K$ so $/K(\alpha)$ so for each such K-homomorphism there are n distinct $K(\alpha)$-homomorphism $K(\alpha, \beta) \to T$ extending it, so there are mn distinct K-homomorphisms $K(\gamma) \to T$, as required.

Example: $K = F_p(x, y), L = K(x^{\frac{1}{p}}, y^{\frac{1}{p}})$ has $[L : K] = [L : K(x^{\frac{1}{p}})][K(x^{\frac{1}{p}}) : K] = p^2$. There is no γ such that $L = K(\gamma)$, as for any $\gamma \in L$ we have $\gamma = \sum_{0 \leq i,j \leq p} a_{ij} x^{\frac{i}{p}} y^{\frac{j}{p}}$ with the $a_{ij} \in K$ so $\gamma^p = \sum a_{ij}^p x^i y \in K$ so $[K(\gamma) : K] \leq p$ and $K(\gamma) \neq L$. Thus we really did need the separability hypothesis in the theorem of the primitive element.

4 Algebraic Closure

Definition: K is algebraicly closed if every nonconstant polynomial $f \in K[x]$ has a root in K (i.e. f splits in K).

Lemma: TFAE: i) K is algebraicly closed, ii) If L/K is an extension with $\alpha \in L$, α algebraic $/K$ then $\alpha \in K$ iii) if L/K is an algebraic extension then $L = K$; these are all obvious.

Example: $\mathbb{C}$ is algebraicly closed, as is $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic } /\mathbb{Q}\}$ - the proof of this is an exercise.

Definition: An extension L/K such that i) L is algebraic $/K$ and ii) L is algebraicly closed is called an algebraic closure of K, e.g. $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Without proof, every field has an algebraic closure L and if L_1, L_2 are two algebraic closures of K then $\exists$ (not generally unique) K-isomorphism $\phi : L_1 \to L_2$; the algebraic closure of K is often denoted $\overline{K}$.

For an example, $\overline{F_p}$: choose a sequence r_i from $\mathbb{N}$ such that $r_i \mid r_i + 1 \forall i$ and for any $n \in \mathbb{N}\exists i$ such that $n \mid r_i$; $r_i = i!$ works fine. Let $F_{(i)} = F_{p^{r_i}}$ so $F_{(1)} \subset F_{(2)} \subset \ldots$. Then let $\overline{F_p} = \bigcup_i F_{(i)}$ (the reason for this construction is to be able to define $\bigcup_i F_{p^i}$ in a meaningful way, since e.g. $F_{p^2} \not\subseteq F_{p^3}$. This is $\overline{F_p}$; it is algebraicly closed, since if $f(x) \in \overline{F_p}[x]$ then f has only finitely many coefficients, so they all lie in some F_q, then we have a splitting field for f, which is finite, $F_{q'}$ for some $q' = q^N$ so f splits in $F_{q'}[x] \subset \overline{F_p}[x]$.

The proof of the above result which we didn't proove is along similar lines: we take a field K and adjoin all roots of polynomials in it to it. Then we adjoin all roots of polynomials over this field to it, and though it might seem that this process would continue indefinitely, we get an algebraicly closed field by set theory set theory mohammed jihad. The axiom of choice is invoved.

5 Galois Extensions

So far we have considered the properties of $\frac{K(\alpha)}{K}$ only in terms of the properties of a single root α of f, where f is the minimal polynomial of α. Recall $K[\alpha] = \frac{K[x]}{(f)}$. Now we want to understand all the roots of f, and the relations between them; in particular, the nonuniqueness of isomorphisms.

Definition: For L/K a field extension, $\mathrm{Aut}(L/K)$ = the set of $\phi : L \to L$ field homomorphisms which are isomorphisms, such that $\phi \mid_K = 1$, i.e. the set of K-homomorphisms which are isomorphisms. This [group] exactly captures the failure of isomorphisms to be unique: if $\phi : M \to L$ is a K-isomorphism and $\sigma \in \mathrm{Aut}(L/K)$ then $\sigma\phi$ is another K-isomorphism $M \to L$, and conversely if $\phi_1, \phi_2 : M \to L$ are two K-isomorphisms then $\phi_1\phi_2^{-1} \in \mathrm{Aut}(L/K)$.

Example: Suppose L/K has degree 2, so $L = K(\alpha)$ for any $\alpha \in L \setminus K$. So if the minimal polynomial of α is $f(x) = x^2 + bx + c = (x-\alpha)(x-\alpha')$ in a splitting field for f, but we have $\alpha + \alpha' = b, \alpha\alpha' = c$. As $\alpha \in L$, $\alpha' = b - \alpha \in L$, so L is a splitting field for f and $L = K(\alpha')$ also. Now by the key lemma, the K-homomorphisms $K(\alpha) \to L$ biject with the roots of f in L, so there is a K-homomorphism $\sigma : K(\alpha) = L \to K(\alpha') = L$ sending $\alpha \mapsto \alpha'$; we then have $\sigma(\alpha') = \sigma(b - \alpha) = b - \alpha' = \alpha$, so σ switches the roots of f. So $\sigma : L \to L$ is a field automorphism and a K-homomorphism, i.e. $\sigma \in \mathrm{Aut}(L/K)$, and by the key lemma there are no other non-identity elements of $\mathrm{Aut}(L/K)$. So the only remaining question is whether $\sigma = 1$, but if $\alpha = \alpha'$ then $2\alpha = \beta$, so assuming char$K \neq 2$ this implies $\alpha = \frac{\beta}{2} \in K$, contradicting $\alpha \in L \setminus K$ so $\sigma \neq 1$; if char$K \neq 2$ then a quadratic field extension (i.e. one with $[L : K] = 2$) has $\mathrm{Aut}(L/K) = \frac{\mathbb{Z}}{2}$. Examples are $\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})$ or $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$, with generator $a+bi \mapsto a-bi$, or $\mathrm{Aut}(\mathbb{Q}(1+\sqrt{2})/\mathbb{Q})$ with generator $\sigma : a+b(1+\sqrt{2}) \mapsto a+b(1-\sqrt{2})$, i.e. $c + d\sqrt{2} \mapsto c - d\sqrt{2}$, since $1 \pm \sqrt{2}$ are the roots of the minimal polynomial of $1 + \sqrt{2}$. Note that this σ is not continuous when we consider $\mathbb{Q}(1+\sqrt{2})$ as a subfield of $\mathbb{R}$; these symmetries do not respect the topology of the embedding.

If char$K = 2$ then $\mathrm{Aut}(L/K) = \frac{\mathbb{Z}}{2} \Leftrightarrow \{\alpha^2 : \alpha \in L\} \neq K$.

Example: $L/K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$; the minimal polynomial $f(x) = x^3-2 = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)$ is its factorization over $\mathbb{C}$, where $\omega = e^{\frac{2\pi i}{3}}, \alpha = \sqrt[3]{2}$. $\omega\alpha, \omega^2\alpha \notin L$ so the key lemma implies since $f(x)$ has only one root in L, $\mathrm{Aut}(L/k) = \{1\}$.

Example: $L = K(x)$, rational functions in one variable over K. It is an exercise to find that $\mathrm{Aut}(L/K) = PGL_2(K) := \frac{SL_2(K)}{\text{scalar matricies}}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \frac{ax+b}{cx+d}$ (i.e. möbius transforms); it is clear that these transforms are all field automorphisms, so the exercise lies in showing that there are no others.

If $[L : K] = \infty$ then $\#\mathrm{Aut}(L/K)$ is also infinite. [Lecturer wrote if $\#K = \infty$ then..., but that's bollocks].

Example: L/K such that $[L : K] = 4, \mathrm{char} K \neq 2$. L is generated $/K$ by two elements of degree 2, called a "biquadratic" field extension; $L = K(\alpha, \beta)$ with $K(\alpha), K(\beta)$ quadratic (we will take quadratic extensions to implicitly mean they are separable). So $\alpha^2 + b\alpha + c = 0$ for some $b, c \in K \therefore \alpha = \frac{-b\pm\sqrt{D}}{2}$ where $D = b^2 - 4ac$; replacing α by $\sqrt{D}$ (since $K(\sqrt{D} = K(\alpha))$ we can wlog take the minimial polynomial of α to be $x^2 - D$. Now $\mathrm{Aut}(K(\sqrt{D})/K) = \frac{\mathbb{Z}}{2}$ generated by $\sigma : \sqrt{D} \mapsto -\sqrt{D}$. Say $\alpha^2 = a, \beta^2 = b$, then we have a unique $K(\alpha)$-isomorphism $L \to L$ by $\beta \mapsto -\beta$, called σ_β, and similarly σ_α. Then $\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha, \sigma_\alpha^2 = 1 = \sigma_\beta^2$ so $\mathrm{Aut}(L/K) \supset \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$. Now by the key lemma any K-automorphism of L must permute the roots of $x^2 - a$ and also the roots of $x^2 - b$, but if $\phi : L \to L$ fixes α, β then it fixes all of L pointwise. So $\mathrm{Aut}(L/K) \subset \mathrm{Sym}(2) \times \mathrm{Sym}(2) = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$ and $\mathrm{Aut}(L/K) = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$.

Lemma: i) for L/K a field extensions, $f \in K[x], \sigma \in \mathrm{Aut}(L/K), \alpha \in L$ is a root of f iff $\sigma\alpha$ is, ii) If $L = K(\alpha_1, \ldots, \alpha_n), \sigma \in \mathrm{Aut}(L/K)$ such that $\sigma\alpha_i = \alpha_i \forall i$ then $\sigma = 1$ (these two are obvious from the above), and iii) if L is a splitting field for f then $\mathrm{Aut}(L/K) \subset \mathrm{Sym}\{\alpha_1, \ldots, \alpha_r\}$ the group of permutations of r letters, where the α_r are the distinct roots of f; this follows from the first two parts.

This lemma raises the question: which subgroup of $\mathrm{Sym} r$ is $\mathrm{Aut}(L/K)$?

Example: For L/K biquadratic, L is a splitting field for $(x^2 - a)(x^2 - b)$ so $\mathrm{Aut}(L/K) = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2} \subsetneq \mathrm{sym}_4$.

Not every field extension is a splitting field, e.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, so there is some content to the following:

Theorem: For L/K a finite extension, $\mathrm{Aut}(L/K)$ is finite; $K(x)/K$ shows that we do need the hypothesis. As one proof, we have $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in L$; let $f_1, \ldots, f_n$ be the respective minimal polynomials of $\alpha_1, \ldots, \alpha_n$ and M a splitting field for $f_1 f_2 \ldots f_n$, then if $\sigma \in \mathrm{Aut}(L/K)$ then σ permutes the roots of each f_i by the above lemma, and conversely if σ fixes the roots of each f_i then it fixes the α_i so is the identity on L, i.e. $\mathrm{Aut}(L/K) \subset \prod \mathrm{sym}_{\deg f}$ so is finite.

An alternative proof: we shall never use this, but the proof contains useful ideas:

Theorem: For L/K a finite extension, $\#\mathrm{Aut}(L/K) \leq [L : K]$; in particular $\mathrm{Aut}(L/K)$ is finite. We shall below proove $\#\mathrm{Aut}(L/K) \mid [L : K]$ without reference to this result, so this theorem is truly useless. We shall deduce it from the following:

Proposition (Linear Independence of Characters): Let Γ be a group, possibly infinite, L a field and $\sigma_1, \ldots, \sigma_n : \Gamma \to L^\times$ distinct group homomorphisms. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent over L, i.e. if $y_1, \ldots, y_n \in L$ are such that $\sum y_i\sigma_i(g) = 0 \forall g \in \Gamma$ then $y_i = 0 \forall i$ (this is a special case of a theorem in representation theory): suppose not and let n be minimal for such a relation to exist; clearly we have $n \geq 2$ and $y_i \neq 0 \forall i$. Since $\sigma_1 \neq \sigma_2$, $\exists g \in \Gamma$ such that $\sigma_1(g) \neq \sigma_2(g)$, then $\forall h \in \Gamma$, $\sum y_i\sigma_i(gh) = \sum y_i\sigma_i(g)\sigma_i(h) = 0$; multiplying $\sum y_i\sigma_i = 0$ by $\sigma_1(g)$ we have $\sum y_i\sigma_1(g)\sigma_i(h) = 0$, but subtracting, $\sum_{i=2}^n y_i(\sigma_i(g) - \sigma_1(g))\sigma_i(h) = 0 \forall h$

and this is a shorter relation, a contradiction.

Proof of the above theorem: $\mathrm{Aut}(L/K) \subset$ the set of K-linear vector space maps $\phi : L \to L$; this is a vector space over K but also over L by $(l\phi)(x) = l(\phi(x))$; the dimension of this is $[L : K] = n$ (we have a basis by $\delta_i : x_j \mapsto \delta_{ij}$), so the theorem implies $\#\mathrm{Aut}(L/K) \leq \dim_L$ of this vector space, which is n.

This is the most important piece of theory in the course: suppose we have a polynomial over a field. Can we find its roots? Somewhat weaker, can we find its splitting field? We shall see that $\mathrm{Aut}(L/K)$ controls the field extension, and more; it controls finding the roots; in fact it tells us [almost] everything.

Let L be a field, $G \subset \mathrm{Aut}(L/K)$ a finite subgroup (e.g. $G = \mathrm{Aut}(L/k)$ for L/K a finite extension). Then:

Definition: $L^G = \{l \in L : gl = l \forall g \in G\}$ the fixed field or field of invariants; prooving this is a field is a trivial exercise. An example is for $L = \mathbb{Q}(i), G = \frac{\mathbb{Z}}{2}$ spanned by $\sigma : i \mapsto -i$ we have $L^G = \mathbb{Q}$.

Write $K = L^G$, then we ask what we can say about L/L^G. For examule, for $L = K(y)$ the field of rational functions and G a finite subgroup of $PSL_2(K)$, what is L/L^G?

Lemma: every $\alpha \in L$ has degree $\leq \#G$ over K; in particular L/K is an algebraic extension. Set $f(x) = \prod_{\sigma \in G}(x - \sigma\alpha) \in L[x]$, then $\deg f = \#G, f(\alpha) = 0$. G acts on L so acts on $L[x]$ by $\sigma(\sum \alpha_i x^i) = \sum \sigma(\alpha_i)x^i$. Each $\sigma : L[x] \to L[x]$ is a ring homomorphism: $\sigma(f + g) = \sigma(f) + \sigma(g), \sigma(fg) = \sigma(f)\sigma(g)$, and $(L[x])^G = L^G[x]$ $(= K[x])$. But $\tau f(x) = \prod_{\sigma \in G} \tau(x - \sigma\alpha) = \prod_{\sigma \in G}(x - \tau\sigma(\alpha)) = \prod_{\sigma \in G}(x - \sigma\alpha) = f(x) \forall \tau \in G$, as $\sigma \mapsto \tau\sigma$ is a bijection of G. So $f(x) \in (L[x])^G = L^G[x]$.

Lemma: L/L^G is separable: let $\alpha \in L$, then must show that the minimal polynomial of α/L^G has distinct roots. Let $\{\sigma\alpha : \sigma \in G\} = \{\alpha_1, \ldots, \alpha_r\}$ be the orbit of α under G (with the α_i distinct). Set $g(x) = \prod_{i=1}^r (x - \alpha_i)$, then we have $g(\alpha) = 0$ and g has distinct roots, but we also have $\sigma g(x) = g(x) \forall \sigma \in G$ as any such σ permutes the α_i. So $g(x) \in L^G[x]$, so the minimal polynomial f of α/L^G divides g so has distinct roots.

Lemma: let $\alpha \in L$, then the minimum polynomial of α is $g(x) = \prod_{\beta \in G\alpha}(x - \beta)$ where $G\alpha$ is the orbit of α under G as above; in particular $\deg \alpha = \#G\alpha$: we have already seen the minimal polynomial divides g so we just need that g is irreducible: if we had $g = f_1 f_2$ for some $f_i \in L^G[x]$ then in $L[x]$, $g(x) = (x - \alpha_1) \ldots (x - \alpha_r)$ so $f_1(x) = \prod_{\alpha_i \in A}(x - \alpha_i), f_1(x) = \prod_{\alpha_i \in B}(x - \alpha_i)$ for some partition of $G\alpha$ as $A \cup B$. But since $f_i(x) \in L^G[x] = (L[x])^G$, G permutes the roots of each f_i, i.e. $GA = A, GB = B$, but since $A \cup B$ is a single orbit we must have one of A, B empty and we have the result.

Example: let $L = \mathbb{Q}(i, \sqrt{2}), G = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2} = \mathrm{Aut}(L/K)$ where $K = \mathbb{Q}$; note that here $L^G = K$ [this is not always the case]. If $\gamma = i, G_i = \{\pm i\}$ so the minimal polynomial is $(x - i)(x + i) = x^2 - 1$; if $\gamma = 1 + i + \sqrt{2}$, the minimal polynomial is $(x - 1 - i - \sqrt{2})(x - 1 + i - \sqrt{2})(x - 1 - i + \sqrt{2})(x - 1 + i + \sqrt{2})$ (which we can calculate as a polynomial over $\mathbb{Q}$.

Now we have two algorithms for computing the minimal polynomial of $\gamma \in L$; we can comupte $1, \gamma, \ldots, \gamma^{[L:K]}$ and look for a linear relation, or use $\prod_{\beta \in G\gamma}(x - \beta)$; it should be clear that this second method is both faster and nicer, since it "tells us more about what's really going on".

Proposition: L/L^G is a finite extension: choose $\alpha \in L$ such that $[K(\alpha) : K]$ is mayimal; it is $\leq \#G$ by the first of the three Lemmas above. Take $\beta \in L$; we shall show that any such is $\in K(\alpha)$ (i.e. $K(\alpha) = L$): β is algebraic over K

so also over $K(\alpha)$, so $[K(\alpha,\beta) : K(\alpha)]$ is finite; we then have $[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K]$ finite; α,β are separable over K so by the theorem of the primitive elemnte $K(\alpha,\beta) = K(\gamma)$ for some $\gamma \in K(\alpha,\beta)$ so $K \subset K(\alpha) \subset K(\gamma$, and $[K(\gamma) : K] \geq [K(\alpha : K]$ but $[K(\alpha) : K]$ is maximal so $[K(\gamma) : K] = [K(\alpha) : K]$ and $K(\gamma) = K(|alpha)$ so $\gamma \in K(\alpha)$ [so $\beta \in K(\alpha)$.

Theorem (Artin): Assume L is a field and $G \leq \mathrm{Aut}(L)$ finite, then i) $[L : L^G] = \#G$ and ii)$\mathrm{Aut}(L/L^G) = G$: set $K = L^G$, then by the above proposition $L = K(\gamma)$ or some γ and $\deg\gamma = \#G\gamma$ so we need $\#G\gamma = \#G$, i.e. $\mathrm{stab}_G\gamma = 1$, but every $\sigma \in \mathrm{stab}_G\gamma$ acts trivially on $K(\gamma)[= L]$ but since $G \subset \mathrm{Aut}(L)$, nontrivial elements of G act nontrivially on L and we have the result. We could also have finished this proof by saying $[L : L^G] \leq \#G$ by the proposition above but $\#G \leq [L : K]$ by linear independence of field automorphisms: but this is very much overkill. For the second part of the theorem, we have $G \leq \mathrm{Aut}(L/K)$ and want to show equality: $L^{\mathrm{Aut}(L/K)} \subset L^G$ but $L^G = K$ with $K \subset L^{\mathrm{Aut}(L/K)}$ by the definition of $\mathrm{Aut}(L/K)$, so $L^{\mathrm{Aut}(L/K)} = L^G = K$. So by the first part, $[L : L^{\mathrm{Aut}(L/K)}] = \#\mathrm{Aut}(L/K) = [L : L^G] = \#G$ so $G = \mathrm{Aut}(L/K)$.

This theorem is useful for computing examples, e.g. $L = \mathbb{C}(y), G = \langle\sigma,\tau\rangle$ where $\sigma y = \frac{i}{y}, \tau y = -y$. What is L^G? First we work out what G is: $\sigma^2 y = \frac{i}{\frac{i}{y}} = 1, \tau^2 y = y, \sigma\tau = \tau\sigma : y \mapsto -\frac{i}{y}$, so $G = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$. The orbit of y under G is $\{y, \frac{i}{y}, -y, -\frac{i}{y}\}$; set $K = L^G$, then the minimal polynomial of y/K is $(x-y)(x+y)(x-\frac{i}{y})(x+\frac{i}{y}) = (x^2+y^2)(x^2+\frac{1}{y^2}) = x^4 + (y^{-2} - y^2)x^2 - 1$; set $w = y^2 - y^{-2}$; since the coefficients of this minimaly polynomial must be $\in K$, $w \in K$ (or we can check it is invariant under the actions of G), so $\mathbb{C}(w) \subset K = L^G \subset L = \mathbb{C}(y)$; by Artim, $[L : L^G] = 4$, but we have just shown the minimal polynomial of y over $\mathbb{C}(w)$ has degree 4, so $K = \mathbb{C}(w)$.

In fact there is Luroth's theorem: for $\mathbb{C} \subsetneq K \subset \mathbb{C}(y)$, $\exists w \in \mathbb{C}(y)$ such that $K = \mathbb{C}(y)$. This theorem is proven in a course on algebraic curves which should appear in part II but does not this year, or in one on Riemann surfaces; essentially it says that the only curve of genus 0 is $\mathbb{P}^1$.

Lemma: $\mathrm{Aut}(F_{q^n}/F_q) = \frac{\mathbb{Z}}{n}$ (where $q = p^k$ as usual): let $\phi(x) = x^q$, then $\phi \in \mathrm{Aut}(F_{q^n}/F_q)$ (ϕ is the kth power of the "Frobenius" ring homomorphism $x \mapsto x^p$); this gives us a map $\mathbb{Z} \to \mathrm{Aut}(F_{q^n}/F_q)$ by $i \mapsto \phi^i$. It is clear that $n \mapsto \phi^n = \mathrm{Id}$, and if $0 < i < n$ then $\phi^i(x) \neq x$ for some $x \in F_{q^n}$, as $(F_{q^n})^{\phi^i}$ the set of fixed points of the field under ϕ^i is F_{q^i}. So we have an injective map $\frac{\mathbb{Z}}{n} \to \mathrm{Aut}(F_{q^n}/F_q)$ which is also surjective, either by the fact that $\#\mathrm{Aut}(F_{q^n}/F_q) \leq [F_{q^n} : F_q] = n$ by linear independence of characters, or immediately from Artin's theorem since $F_{q^n}^{\frac{\mathbb{Z}}{n}} = F_q$.

Definition: An extension L/K is Galois if i) L/K is finite and ii) $K = L^{\mathrm{Aut}(L/K)}$. If L/K is Galois we call $\mathrm{Aut}(L/K)$ its Galois group.

For $G \subset \mathrm{Aut}(L)$, L/L^G is Galois; by Artin this means Galois extensions L/K are separable.

Theorem L/K is Galois iff L is a splitting field for a separable polynomial over K; we shall proove this just below.

Proposition: For L/K a finite extension, $\#\mathrm{Aut}(L/K) \mid [L : K]$ with equality iff L/K is Galois: set $M = L^{\mathrm{Aut}(L/K)}$, then $K \leq M \leq L$, so $[L : M] = \#\mathrm{Aut}(L/K)$ by Artin. So by the tower law $[L : K] = [M : K]\mathrm{Aut}(L/K)$.

Theorem, including the above unproven statement: TFAE: i) L/K Galois, i.e. L/K is finite and $\forall l \in L \setminus K \exists \sigma \in \mathrm{Aut}(L/K) : \sigma l \neq l$. ii) $\exists$ a finite subgroup $G \subset \mathrm{Aut}(L)$ such that $K = L^G$. iii) L is the splitting field of a separable polynomial iv) L/K is separable and the minimal polynomial of each $\alpha \in L$ splits into linear factors in L. That i) implies ii) is trivial and the converse to this is by Artin; we saw that ii) implies iv) in the proof of Artin (the linear factors have roots $\{g\alpha : g \in G\}$). ii) trivially implies iv): if $L = K(\alpha_1, \ldots, \alpha_n)$ let f_i be the minimal polynomial of each α_i, then the lcm of these f_i is separable and L is its splitting field. Finally iii) implies i): if L is the splitting field of a separable polynomial f, then by the umiqueness of splitting fields and our key lemma, far above, there are $[L : K]$ K-homomorphisms $L \to L$, i.e. $\#\mathrm{Aut}(L/K) = [L : K]$ and we are done by the above proposition.

Corollary: any finite separable extension L/K is contained in a Galois extension: $K \leq L \leq N$ with N/K Galois: if $L = K(\alpha_1, \ldots, \alpha_n)$, then let N be the splitting field of the lcm of the minimal polynomials of the α_i, which is separable, and by the above theorem N/K is Galois. Moreover, no proper subfield of this N is Galois (this is an exercise); if $K \leq L \leq N'$ is an extension such that N'/K is Galois but no proper subfield therof is, then $\exists$ an L-isomorphism $N \to N'$ (by uniqueness of splitting fields).

Corollary: If $K \leq M \leq L$ are field extensions and L/K Galois then L/M is Galois; properties iii) and iv) in the above theorem hold for L/K so they hold for L/M.

Fundamental Theorem of Galois Theory

Let L/K be a Galois extension, $G = \mathrm{Aut}(L/K)$. Then there is a bijection between subgroups of G and fields M with $K \leq M \leq L$ (called intermediate subfields), $H \mapsto L^H$ with inverse $M \mapsto \mathrm{Aut}(L/M)$; in particular this means there are only finitely many intermediate subfields. To proove this it is enough to check that both compositions of the two maps are identities; $H \mapsto L^H \mapsto \mathrm{Aut}(L/L^H)$ is the identity as $\mathrm{Aut}(L/L^H) = H$ by Artin, and $M \mapsto \mathrm{Aut}(L/M) \mapsto L^{\mathrm{Aut}(L/M)}$ is also the identity since L/M is Galois by the above corollary, so $L^{\mathrm{Aut}(L/M)} = M$.

Example: $L = F_{q^n}, K = F_q, G = \mathrm{Aut}(F_{q^n}/F_q) = \frac{\mathbb{Z}}{n}$: the subgroups of $\frac{\mathbb{Z}}{n}$ biject with the intermediate subfields; such subgroups are given by integers m dividing n, then $L^{\langle \phi^m \rangle} = F_{q^m}$ - but we knew this already.

Example: $L = \mathbb{Q}(i, \sqrt{2}), \mathbb{Q} = K, G = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2} = \langle \sigma, \tau \rangle$ where $\sigma : i \mapsto -i, \tau : \sqrt{2} \mapsto -\sqrt{2}$. We have subgroups $1, \langle \sigma \rangle, \langle \tau \rangle, \langle \sigma\tau \rangle, \langle \sigma, \tau \rangle$; these correspond respectively to $\mathbb{Q}(i, \sqrt{2}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{2}), \mathbb{Q}[$, so these are precisely the intermediate field extensions].

Some properties of the bijection between subgroups of G and intermediate fields M in the FTGT: it is order reversing ($H' \leq H \Rightarrow L^{H'} \geq L^H$, $M \leq M' \Rightarrow \mathrm{Aut}(L/M') \leq \mathrm{Aut}(L/M)$. Less obviously, L^N/K is Galois iff $N \triangleleft G$ (the notation is "is a normal subgroup of"), and in this case $\mathrm{Aut}(L^N/K) = \frac{G}{N}$; this is plausible, since we have $L/M/K$ with $[L : K] = \#G = \#\mathrm{Aut}(L/K), [L : M] = \#H = \#\mathrm{Aut}(L/M)$, and $[M : K] = \frac{\#G}{\#H}$, which of course would be $\#\frac{G}{H}$ but there is a quotient group $\frac{G}{H}$ iff H is normal. To proove the result, suppose $N \triangleleft G$, and put $M = L^N$; observe that for $\sigma \in G$, $\sigma M = M$ since if $l \in M, n \in N$ then n fixes σl, as $n\sigma l = \sigma\sigma^{-1}n\sigma l = \sigma n' l$ for some $n' \in N$, since N is normal, but $n'l = l$ as $l \in L^N = M$. So G acts on M, i.e. we have a map $G \to \mathrm{Aut}(M/K)$), but the set of $\sigma \in G$ for which the restriction to L^N is the identity is $\mathrm{Aut}(L/L^N)$, the kernel of this map, which $= N$ by Artin, so $\frac{G}{N}$ injects into $\mathrm{Aut}(M/K)$; $[L : L^N] = \#N, [L^N : K] = \#\frac{G}{N}, \#\mathrm{Aut}(L^N/K) \leq \#\frac{G}{N}$ but the left hand side is $\frac{G}{N}$ so we have equality and the extension is Galois as required.

For the converse, suppose $K \subset M \subset L, M = L^H$ for $H = \mathrm{Aut}(L/M()$. Suppose M/K Galois, then M is the splitting field of some separable polynomial f/K, so for $\sigma \in G = \mathrm{Aut}(L/K)$, if σ permutes the roots of f then $\sigma M = M$. But $\mathrm{Aut}(L/\sigma M) = \sigma\mathrm{Aut}(L/M)\sigma^{-1}$, since g is a member of the left hand side ifff $g\sigma M = \sigma M \Leftrightarrow \sigma^{-1}g\sigma M = M$, which is the case iff $\sigma^{-1}g\sigma \in \mathrm{Aut}(L/M)$, so since σ fixes M, $\sigma H \sigma^{-1} = H \forall \sigma \in G$, i.e. $H \triangleleft G$.

Definition: If $f \in K[x]$ is a separable polynomial (where we consider a reducible polynomial to be separable iff its irreducible factors are), the Galois group of f $\mathrm{Gal}_K(f) = \mathrm{Aut}(L/K)$ where L is a splitting field for f/K; uniqueness of splitting fields implies this is well defined.

Suppose we ask: what is $\mathrm{Gal}_{\mathbb{Q}}(x^3 - 3x + 1)$? Or, weaker, what is f's splitting field?

Lemma: for $f \in K[x]$ separable, f is irreducible iff $\mathrm{Gal}(f)$ acts transitively on the roots of f: let L be a splitting field, $\{\alpha_1, \dots, \alpha_r\}$ the roots of f in L; write this set as a disjoint union $X_1 \amalg \cdots \amalg X_k$, where each X_i is a single orbit under G. Put $f_i = \prod_{\alpha_j \in X_i}(x - \alpha_j)$ so $f = f_1 \dots \cdot_k$, and each $f_i \in K[x]$ has $\sigma f_i = f_i \forall \sigma \in G$.

An extended example: cubics. Let $f \in K[x]$ be an irreducible separable cubic $f(x) = x^3 + ax^2 + px + q$, let L be a splitting field so $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in L[x]$, so expanding $\alpha_1 + \alpha_2 + \alpha_3 = -a, \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p, \alpha_1\alpha_2\alpha_3 = -q, L = K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2) = K(\alpha_2, \alpha_3) = K(\alpha_3, \alpha_1)$ since $\alpha_3 = a - \alpha_1 - \alpha_2$ and similarly. So we have a tower of fields $K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) = L$, with $[K : K(\alpha)] = 3$ as f is irreducible. So there are two possibilities: either $K(\alpha_1) = K(\alpha_1, \alpha_2)$ in which case $[L : K] = 3$, or $K(\alpha_1) \neq K(\alpha_1, \alpha_2)$, impyling the quadratic polynomial $(x - \alpha_2)(x - \alpha_3) = \frac{f(x)}{x - \alpha_1} \in K(\alpha_1)[x]$ is irreducible, so $[L : K(\alpha_1)] = 2 \therefore [L : K] = 3 \times 2 = 6$. observe that if $[L : K] = 3$ there are no intermediate field extensions; we knew this already since p is prime, but now we have a "better" and generalizable reason: the FTGT, as $\frac{\mathbb{Z}}{3}$ has no subgroups.

Now we shall determine $G = \mathrm{Gal}(f)$ and all intermediate subfields: for $\deg F = 3, G \subset S_3$; the subgroups of $S{-}3$ are 1, three copies of $\frac{\mathbb{Z}}{2}$ by $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$, $\frac{\mathbb{Z}}{3} = \langle(123)\rangle = H = A_3$ and S_3 itself; from the above G acts transitively on $\{1, 2, 3\}$ so the only possibilities are $G = A_3$ (in which case $[L : K] = 3$) and $G = S_3$ (in which case $[L : K] = 6$); in the first case there are no intermediate subfields and nothing to say, but if $G = S_3$ we have something new: we know what the subgroups of S_3 are. Consider $L^{\langle(23)\rangle}$; $(23) : \alpha_2 \mapsto \alpha_3, \alpha_3 \mapsto \alpha_2$, so $K \subset K(\alpha_1) \subset L^{\langle(23)\rangle} \subset L$; by Artin $[L^{\langle(23)\rangle} : L] = 2$ and we know $[K(\alpha) : K] = 3$ so $L^{\langle(23)\rangle} = K(\alpha_1)$; similarly we have 1 corresponds to L, (12) to $K(\alpha_3)$, (23) to $K(\alpha_1)$, (31) to $K(\alpha_2)$, S_3 to K, and $A_3 = H$ to some new subfield: $K \leq L^H \leq L$; $[L : L^H] = 3$ so $[L^H : K] = 2$; we have a unique subfield M such that $[M : K] = 2$ i.e. M is quadratic. So $M = K(\sqrt{D})$ for some $D \in K$ (assuming $\mathrm{char}K \neq 2$), i.e. we have a $\delta \in L$ such that $\delta^2 = D \in K, H\delta = \delta$ (i.e. $(123)\delta = \delta$), but $(12)\delta \neq \delta$ and similarly.

Suppose we have this case: $G = S^3$ so we have $K \subset M \subset L$ where $M = L^{A_3}$, with $[M : K] = 2, [L : M] = 3$ i.e. M/K is a quadratic extension (we have M/K Galois since $A_3 \triangleleft S_3$, but we knew this already since it is a quadratic extension). So we look for $\delta \in L \setminus K$ such that $M = K(\delta)$; we assume $\mathrm{char}K \neq 2$. We want $(12)\delta \neq \delta, (123)\delta = \delta$. It would be nice to have $\delta^2 = D \in K$ (and in fact we shall do so). We observe that $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ has these properties;

$(12)\delta = -\delta$ [$\neq \delta$, since char$K \neq 2$], so $\delta^2 = D$ is fixed by all of S^3 su must be $\in K$. $D = 0 \Leftrightarrow \alpha_i$ distinct, i.e. f is separable (recall we assume f irreducible; we haven't yet proven $D \in K$ if f is not separable, but we shall do so, and it is reasonable; informally the δ we have defined "should" detect separability).

We have shown that $[L : K] = 6 \Rightarrow D$ is not a square in K, as $M = K(\sqrt{D})$ is the unique subfield of L with M/K quadratic (by FTGT). But conversely, if $[L : K] = 3$ then D as we have defined it must be a square, as $\sqrt{D} = \delta$ is fixed by $A_3 = \langle(123)\rangle = \text{Aut}(L/K)$ so $\delta \in K$.

Therefore, "we win"; we have a useful result, because we can compute $D = \delta^2$ from f without having to first find the roots $\alpha_1, \alpha_2, \alpha_3$ of f; the reader may verify that $D = a^2p^2 - 4p^3 - 4a^3q - 27q^2 + 18apq$; this is too "messy" to easily remember, but if $a = 0$ then we have the much nicer form $D = -4p^3 - 27q^2$, so if char$K \neq 3$ we consider $g(x) = f(x - \frac{a}{3})$ which has the same splitting field as f but no coefficient of x^2. D is called the "discriminant".

Corollary: suppose char$K \neq 2, f(x) = x^3 + px + q \in K[x]$ irreducible. Let $D = -4p^3 - 27q^2 \in K$; then f is separable iff $D \neq 0$, and [in this case] $\text{Gal}(f) = S_3$ if $\sqrt{D} \notin K$ or A_3 if $\sqrt{D} \in K$.

An example: $K = \mathbb{Q}, f(x) = x^3 - 2$; we have $D = -27 \times 2^2 = -3^3 \times 2^2 < 0$ which is not a square, so $G = S_3$ (as we knew already). $f(x) = x^3 - 3x^2 + 1$ has $D = -4 \times -27 - 27 = 3^4$ which is a square (in $\mathbb{Q}$), so $\text{Gal}(f) = A_3$; $f(x) = 3x^2 + 1$ has $D = -5 \times 3^3 < 0$ which is not a square, so $\text{Gal}(f) = S_3$.

Remark: if $f(x) \in \mathbb{Q}[x]$ has only one real root, then its splitting field has degree 6; this is obvious since adjoining the real root of f could not give the complex roots, but can also be shown (and this is an exercise) by computing D and checking it is not a square. This is useful as if we have $f'(x) > 0 \forall x \in \mathbb{R}$ (e.g. $f(x) = x^3 + 3x + 1$) then we know f is increasing in x so has at most 1 real root.

We can of course proove that our above expression for D is valid by simply expanding it, but can we find one in general? Informally, one must exist, because D is a function of the α_i invariant under S_3, so must be some function of a, p, q; more formally:

Proposition: For K a field with char$K \neq 2, f \in K[x]$ irreducible, and L a splitting field for f, let $f(x) = \prod(x - \alpha_i)$ in $L[x]$. Then: i) $D \in K$ and $D \neq 0 \Leftrightarrow f$ separable, ii) D is a square in $K \Leftrightarrow \text{Gal}(f) \subset A_n$, iii) D is a polynomial in the coefficients of f. For the first two parts, put $\delta = \prod_{i<j}(\alpha_i - \alpha_j) \in L$, so $\delta^2 = D$, and let $G = \text{Gal}(f) \subset S_n$; it is clear that $\delta \neq 0 \Leftrightarrow f$ is separable, and if $\sigma \in G$ we have $\sigma\delta = -\delta$ for $\sigma \notin A_n$ and δ for $\sigma \in A_n$, so $G \subset A_n \Leftrightarrow \sigma\delta = \delta \forall \delta \in G \Leftrightarrow \delta \in L^G = K \Leftrightarrow D = \delta^2$ is a square in K. We shall now proove the third part much more slowly:

6 Symmetric Polynomials

Let R be a ring (e.g. $\mathbb{Z}$), $R[z_1, \ldots, z_n]$ the polynomial ring in n variables over R. S_n acts on this by permuting variables: $wz_i = z_{w(i)}$ for any $w \in S_n$, e.g. $(123)z_1^3z_2z_4^7 = z_{(123)1}^3z_{(123)2}z_{(123)4}^7 = z_2^3z_3z_4^7$. Define the symmetric polynomials by $R[z_1, \ldots, z_n]^{S_n} = \{f \in R[z_1, \ldots, z_n] : wf = f \forall w \in S_n\}$, i.e. f is symmetric if $f(z_1, \ldots, z_n) = f(z_{w1}, \ldots, z_{wn}) \forall w \in S_n$. Examples are the "elementary symmetric polynomials": $e_1 = z_1 + \cdots + z_n, e_2 = \sum_{i<j} z_iz_j$ (i.e. $z_1z_2 + z_1z_3 + \cdots + z_1z_n + z_2z_3 + \cdots + z_{n-1}z_n$), and generally $e_k = \sum_{i_1<\cdots<i_k} z_{i_1} \ldots z_{i_k}$.

Theorem: every symmetric polynomial $f \in R[z_1, \ldots, z_n]^{S_n}$ can be written uniquely as a polynomial in $e_1, \ldots, e_n$, i.e. the map $R[e_1, \ldots, e_n] \to R[z_1, \ldots, z_n]^{S_n}$ (where the LHS is just a polynomial ring in n variables) $e_k \mapsto \sum_{i_1 < \cdots < i_k} z_{i_1} \ldots z_{i_k}$ is an isomorphism of rings. For example, $\sum z_i^2 = e_1^2 - 2e_2$; as an exercise the reader should express $\sum z_i^3$ in terms of e_1, e_2, e_3.

Corollary/Application: for K a field, $f \in K[x], L = K(\alpha_1, \ldots, \alpha_n)$ a splitting field for f, if $f(x) = x^n - a_1 x^{n-1} + \cdots \pm a_n = 0$ we have $a_1 = \alpha_1 + \cdots + \alpha_n, \ldots, a_n = \alpha_1 \ldots \alpha_n$, then by the theorem any symmetric function of the roots can be written as a polynomial in the coefficients a_i of f; in particular, for $D = \prod_{i<j}(z_i - z_j)^2 \in \mathbb{Z}[z_1, \ldots, z_n]^{S_n}$ we must have some polynomial $\Delta(e_1, \ldots, e_n) \in \mathbb{Z}[e_1, \ldots, e_n]$ such that $\Delta(z_1 + \cdots + z_n, \ldots, z_1 \ldots z_n) = \prod_{i<j}(z_i - z_j)^2$ [i.e. $\Delta(a_1, \ldots, a_n) = D$].

Claim: for $n = 3$, $\Delta(0, p, q) = -4p^3 - 27q^2$: $\Delta(a, p, q) = \prod_{1 \leq i < j \leq 3}(z_i - z_j)^2$, a homogenous polynomial of degree 6, so a linear combination of $e_1^6, e_1^4 e_2, e_1^3 e_3, e_1 e_2 e_3, e_2^3, e_3^2$ as these are all the monomials of [degree] 6; the only terms not involving e_1 are the last two, so we have $\Delta(0, p, q) = cp^3 + dq^2$ for some c, d; Δ vanishes if there are repeated roots, so consider $(x - \alpha)(x - \alpha)(x + 2\alpha) = x^3 + (-3\alpha^2)x + 2\alpha^3$, so we have $\Delta(0, -3\alpha^2, 2\alpha^3) = 0$ i.e. $c(-3\alpha^2)^3 + d(2\alpha^3)^2 = 0 \Rightarrow -27c + 4d = 0$. Then evaluating Δ at $x^3 - x = x(x-1)(x+1)$ by explicit computation we find it is 4, i.e. $\Delta(0, -1, 0) = 4 \Rightarrow c = -4 \therefore d = -27$.

Now the proof of the theorem: for $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n$ write $z^\lambda = z_1^{\lambda_1} \ldots z_n^{\lambda_n}$, a monomial. Then $\{z^\lambda : \lambda \in \mathbb{N}^n\}$ is a basis of $R[z_1, \ldots, z_n]$. Totally order $\mathbb{N}^n$ by $\lambda < \mu$ if $\lambda_1 < \mu_1$ or $\lambda_1 = \mu_1$ and $\lambda_2 < \mu_2$ or...; this is called lexicographical ordering. Now if λ is such that $\lambda_1 \geq \cdots \geq \lambda_n$ then $\lambda \geq w\lambda \forall w \in S_n$, i.e. every orbit $S_n \tilde{\lambda}$ has a maximal element λ which is $\tilde{\lambda}$ reoordered so that $\lambda_1 \geq \cdots \geq \lambda_n$. So $\{\sum_{\mu \in S_n \lambda} z^\mu | \lambda \text{ has } \lambda_1 \geq \cdots \geq \lambda_n \geq 0\}$ forms a basis of $R[z_1, \ldots, z_n]^{S_n}$ (as this set is precisely the distinct elements of $\{\sum_{\mu \in S_n \lambda} z^\mu\}$).

Now, for surjectivity of our map, let $f \in R[z_1, \ldots, z_n]^{S_n}$. Write $f = cz^\lambda + \sum_{\mu < \lambda}$ [terms in z^μ]; this is $cz_1^{\lambda_1 - \lambda_2}(z_1 z_2)^{\lambda_2 - \lambda_3} \ldots (z_1 \ldots z_{n-1}^{\lambda_{n-1} - \lambda_n}(z_1 \ldots z_n)_n^\lambda +$ remaining terms; since f is symmetric λ has $\lambda_1 \geq \cdots \geq \lambda_n$. But $e_k = z_1 \ldots z_k +$ some terms z^μ with $\mu < (1, \ldots, 1, 0, \ldots, 0)$, so by carefully expanding we can show that the $f = ce_1^{\lambda_1 - \lambda_2} \ldots e_{n-1}^{\lambda_{n-1} \ldots \lambda_n} e_n^{\lambda_n} +$ some terms in z^μ for $\mu < \lambda$.

Now $f - ce_1^{\lambda_1 - \lambda_2} e_2^{\lambda_2 - \lambda_3} \ldots e_{n-1}^{\lambda_{n-1} - \lambda_n} e_n^{\lambda_n}$ is $\in \mathbb{Z}[z_1, \ldots, z_n]^n$ with leading term z^μ for some $\mu < \lambda$, so we induct ($\{\nu : \nu \leq \lambda\}$ is a finite set).

For injectivity, suppose $g \in R[e_1, \ldots, e_n]$ is such taht $g(\sum_i z_i, \sum_{i<j} z_i z_j, \ldots, z_1 \ldots z_n) = 0$ in $R[z_1, \ldots, z_n]^{S_n}$, then we need $g = 0$. Induct on n; the $n = 1$ case is trivial. For $n > 1$, set $z_n = 0$; then observe $e_k \mapsto \sum_{1 \leq i_1 < \cdots < i_k \leq n} z_{i_1} \ldots z_{i_k}$ becomes $\sum_{1 \leq i_1 < \cdots < i_k \leq n-1} z_{i_1} \ldots z_{i_k}$, i.e. $\mathring{e}_K := e_K |_{z_n = 0}$ is "e_K for $n-1$ variables" for $K \leq n-1$, and 0 for $K = n$. So $g(\mathring{e}_1, \ldots, \mathring{e}_{n-1}, 0) \mapsto g(\sum_{1 \leq i \leq n-1} z_i, \ldots, z_1 \ldots z_{n-1}, 0) = 0$; by induction $g(e_1, \ldots, e_{n-1}, 0)$ is the zero polynomial, so $g(e_1, \ldots, e_n) = e_n h(e_1, \ldots, e_n)$ for some $h \in R[e_1, \ldots, e_n]$ with $z_1 \ldots z_n h(\sum_i z_i, \ldots, z_1 \ldots z_n) = 0$ in $R[z_1, \ldots, z_n]^{S_n}$. But $z_1 \ldots z_n$ is not a zero divisor in $R[z_1, \ldots, z_n]$ so we must have $h(\sum z_i, \ldots, z_1 \ldots z_n) = 0$, but we can wlog take g to be of minimal degree such that $g \neq 0$ and $g(\sum z_i, \ldots, z_1 \ldots z_n) = 0$. So $h = 0$.

7 Cyclotomic Extensions

Let L be a field. Define $\mu_n(L) = \{\alpha \in L : \alpha^n = 1\}$, the nth roots of 1 in L. μ_n is a finite subgroup of $L^\times$ (its elements are the roots of $x^n - 1$, so there are at most n of them), so a cyclic group.

Definition: $\xi \in \mu_n$ is a primitive nth root of 1 if the order of ξ is n, $\Leftrightarrow \#\mu_n = n, \mu_n = \{\xi^k : k \in \mathbb{Z}\}$. If ξ is primitive then ξ^k is primitive whenever $\gcd(k, n) = 1$, i.e. $k \in (\frac{\mathbb{Z}}{n})^\times$, since $\gcd(k, n) = 1 \Leftrightarrow kr + sn = 01$ for some r, s, $\Leftrightarrow r = k^{-1} \in \frac{\mathbb{Z}}{n}$.

If L is the splitting field for $x^n - 1$ over some K then $\#\mu_n(L) = n \Leftrightarrow x^n - 1$ is separable $\Leftrightarrow \gcd(x^n - 1, \frac{d}{dx}(x^n - 1) = nx^{n-1}) = 1 \Leftrightarrow n \neq 0$ in K, i.e. char$K \nmid n$ or char$K = 0$ ($\star\star$); we shall assume this is the case.

Definition: the nth cyclotomic extension of K is the splitting field L of $x^n - 1$ over K. Let $G = \mathrm{Aut}(L/K)$; by our assumption ($\star\star$) L/K is separable so Galois, and [so] there exist primitive nth roots of unity in L; let $\xi \in \mu_n(L)$ be primitive, then:

Lemma: i) $L = K(\xi)$: in $L[x]$, $x^n - 1 = \prod_{\alpha \in \mu_n(L)}(x - \alpha) = (x-1)(x-\xi)\ldots(x-\xi^{n-1})$, as all roots of 1 are powers of ξ; L is a splitting field for $x^n - 1$ so $L = K(\xi)$. ii) There is an injective homomorphism $\chi : G \hookrightarrow (\frac{\mathbb{Z}}{n\mathbb{Z}}^{\times}$ by $\chi(\sigma) = \alpha$ where $\sigma\xi = \xi^\alpha$; moreover this χ is independent of the choice of ξ: if $\sigma \in G$, $\sigma\xi$ also has order precisely n, since $(\sigma\xi)^n = \sigma(\xi^n) = 1$. So $\sigma\xi = \xi^\alpha$ for some $\alpha \in (\frac{\mathbb{Z}}{n})^\times$ [$\frac{\mathbb{Z}}{n}$ is this lecturer's notation for the integers modulo n], so χ is well defined. If $\tau \in G$ and $\tau(\xi) = \xi^\beta$ then $\sigma\tau(\xi) = \sigma(\xi^\beta) = (\sigma\xi)^\beta = \xi^{\alpha\beta}$ (as σ, τ are field homomorphisms), so $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ and χ is a group homomorphism. For injectivity, if $\chi(\sigma) = 1$ then $\sigma\xi = \xi$ so since $L = K(\xi$ σ must be the identity. Now for independence of choice of ξ, if ξ' is another primitive nth root of unity, $= \xi^k$ for some $k \in (\frac{\mathbb{Z}}{n})^\times$. Then $\chi(\sigma) = a \Rightarrow \sigma\xi = \xi^a \Rightarrow \sigma(\xi') = \sigma(\xi^k) = \xi^{ka} = (\xi')^a$, so we would have the same result if we defined χ in terms of ξ'. iii) χ is surjective, and hence an isomorphism, iff G acts transitively on primitive nth roots of 1: G acts transitively iff $\forall k \in (\frac{\mathbb{Z}}{n})^\times \exists \sigma \in G : \sigma\xi = \xi^k \Leftrightarrow \chi$ is surjective.

Corollary: G is abelian.

Warning: note that χ need not be surjective in general, e.g. $K = \mathbb{C} \Rightarrow L = \mathbb{C} \Rightarrow G = \{1\}$ so χ is never surjective.

Example: $K = F_q$, char$K \nmid n$, L the splitting field of $x^n - 1$. Claim $\chi : G = \mathrm{Aut}(L/K) \hookrightarrow (\frac{\mathbb{Z}}{n})^\times$ identifies G with the subgroup $\langle q \rangle \subset (\frac{\mathbb{Z}}{n})^\times$ (where by q we of course really mean $q + n\mathbb{Z}$; the lecturer sometimes uses $\bar{q}$ to denote this coset). Proof: $\mathrm{Gal}(L/K) = \langle \phi_q \rangle$ where $\phi_q(x) = x^q \forall x$, the Frobenius map.

Example: $K = \mathbb{Q}, n = p$ prime, $\omega = e^{\frac{2\pi i}{p}}$: $[\mathbb{Q}(\omega) : \mathbb{Q}] = \#(\frac{\mathbb{Z}}{p})^\times$ (Eisenstein), so χ is surjective. [These last two examples not verified - blame my dad]

Definition: $\Phi_n(x) = \prod_{k \in (\frac{\mathbb{Z}}{n})^\times}(x - \xi^k)$, the nth cyclotomic polynomial. If $\sigma \in G$ then σ permutes the primitive nth roots [of 1], so σ fixes $\Phi_n(x)$ and $\Phi_n(x) \in L[x]^G = K[x]$.

Corollary: $\Phi_n(x)$ is irreducible $\Leftrightarrow \chi$ is surjective $\Leftrightarrow [L : K] = \#G = \#(\frac{\mathbb{Z}}{n})^\times$: Φ_n is irreducible iff G acts transitively on the roots of Φ_n, i.e. on primitive roots, but this is part iii) of our lemma above.

If $d \mid n$ then $x^d - 1 \mid x^n - 1$; dividing $x^n - 1$ by all these "obvious" factors we obtain Φ_n, because every $\alpha \in \mu_n$ is a primitive dth root of 1 for precisely one value of $d \mid n$, namely $d = \mathrm{ord}(\alpha)$, and all primitive dth roots of 1 occur. So we can define Φ_n inductively by $x^n - 1 = \phi_n(x) \prod_{d|n, d \neq n} \Phi_d(x)$. Note that this implies

$\Phi_n(x) \in \mathbb{Z}[x]$, so we can regard it as being $\in K[x]$ for any field K.

Theorem: $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible. As an exercise the reader should use Eisenstein to show this where $n = p^k$ for some prime p and integer k (we have already done this for $n = p$). We shall give a proof due to Dedekidnd (1857): recall Gauss' lemma, that if $f \in \mathbb{Z}[x]$ is monic and factors in $\mathbb{Q}[x]$ then it factors in $\mathbb{Z}[x]$. So suppose $\Phi_n(x) = fg$ for some $f, g \in \mathbb{Z}[x]$; we want to show that if ξ is a rooot ff then ξ^a is a root of $f \forall a$ with $(a, n) = 1$, since then all roots of Φ are roots of f and so $g = 1$. Write a as a product of primes p_i; we have $p_i \nmid n$. Then it is enough to show that if ξ is a root of f then ξ^p is a root of f for any prime $p \nmid n$. Suppose this were not the case: ξ^p is a primitive nth root of 1, but $f(\xi^p) \neq 0$, so $g(\xi^p) = 0$, i.e. ξ is a root of $f(x^p)$. So $f(x), g(x^p)$ have a common factor (since they have a common root ξ). Now reduce modulo p; let $\bar{f}(x) = \sum \bar{a}_i x^i \in \frac{\mathbb{Z}}{p}[x]$, where $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$. $f \mapsto \bar{f}$ is then a ring homomorphism (as $\overline{fg} = \bar{f}\bar{g}$), and $\bar{g}(x^p) = (\overline{g(x)})^p$, so $h \mid f \Rightarrow \bar{h} \mid \bar{f}, h \mid g(x^p) \Rightarrow \bar{h} \mid \bar{g}^p$, so some factor of h divides $\bar{g}$, i.e. $\bar{f}, \bar{g}$ have some common factor, so Φ_n has a multible root, but $p \nmid n$ so Φ_n is separable so has no multiple roots, a contradiction.

Corollary: If $K = \mathbb{Q}, L = \mathbb{Q}(\xi)$ where $\xi = e^{\frac{2\pi i}{n}}$, then $[L : K] = \#(\frac{\mathbb{Z}}{n})^\times$ and χ is an isomorphism $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \to \frac{\mathbb{Z}}{n}$.

We shall write $\mathbb{Q}(\xi_n)$ for the nth cyclotomic extension of $\mathbb{Q}$, i.e. the splitting field for $x^n - 1$ over $\mathbb{Q}$; ξ_n is a primitive nth root of 1. We have Φ_n is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \#(\frac{\mathbb{Z}}{n})^\times$. By the fundamental theorem of Galois theory, intermediate subfields $\mathbb{Q}(\xi_n) \supset M \supset \mathbb{Q}$ biject with subgroups $1 \leq H \leq (\frac{\mathbb{Z}}{n})^\times$ by $M = \mathbb{Q}(\xi_n)^H$; since $(\frac{\mathbb{Z}}{n})^\times$ is abelian, its subgroups are all normal so $M/\mathbb{Q}$ is Galois, with Galois group $\frac{(\frac{\mathbb{Z}}{n})^\times}{H}$. This raises two questions: what is the structure of $(\frac{\mathbb{Z}}{n})^\times$ (in particular, what are its subgroups?), and what are the corresponding subfields?

We'll first compute some examples [we shall sometimes write ξ for ξ_n]. If $n = p$ a prime, then $(\frac{\mathbb{Z}}{p})^\times = F_p^\times$ is a cyclic group $\cong \frac{\mathbb{Z}}{p-1}$, so there is a unique subfield for each $k \in \mathbb{N}$ with $k \mid p - 1$. So, example 1: if $p = 5$, $(\frac{\mathbb{Z}}{5})^\times = \frac{\mathbb{Z}}{4}$ and $\exists!$ intermediate subfield of degree 2, generated by $\eta = \xi_5 + \xi_5^{-1} = 2\cos\frac{2\pi}{5} = -1 + \sqrt{5}$, so we have $\mathbb{Q}(\xi_5) \supset \mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{5}) \supset \mathbb{Q}$; in fact we have more generally:

Lemma: For any $n \geq 3$ (which implies $2 \mid \#(\frac{\mathbb{Z}}{n})^\times$, as we shall see in a moment), there is a unique subfield $M \subset \mathbb{Q}(\xi_n)$ such that $[M : \mathbb{Q}] = \frac{\#(\frac{\mathbb{Z}}{n})^\times}{2}$, i.e. $[\mathbb{Q}(\xi_n) : M] = 2$, namely $M = \mathbb{Q}(\eta) = \mathbb{Q}(\cos\frac{2\pi}{n})$ where $\eta = \xi_n + \xi_n^{-1}$: ξ_n is a root of the quadratic polynomial $x^2 - \eta x + 1 \therefore [\mathbb{Q}(\xi) : \mathbb{Q}(\eta)] \leq 2$, but the field automorphism $\xi \mapsto \xi^{-1}$ fixes η but not (for $n \geq 3$) ξ, so this is exactly 2 and we have the result.

Example 2: $n = 7, \mathbb{Q}(\xi_7), \mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) = (\frac{\mathbb{Z}}{7})^\times = \frac{\mathbb{Z}}{6} = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{3}$; let the Galois group be $\langle\sigma\rangle$ and choose $\sigma = 3$, i.e. $(\frac{\mathbb{Z}}{7})^\times = \{1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5\}$. We already know $\eta = \xi_7 + \xi_7^{-1}$ has degree $\frac{6}{2} = 3$ over $\mathbb{Q}$; let's write down its characteristic polynomial. Artin tells us to consider the orbit of η under G; we know σ^3 fixes η, as $\frac{\mathbb{Z}}{2} = \langle\sigma^3\rangle$ and $\eta \in \mathbb{Q}(\xi_7)^{\frac{\mathbb{Z}}{2}}$ (and we can see $\sigma^3(\xi) = \xi^{-1}$, so this is right); the orbit is $\{\eta = \xi + \xi^{-1}, \sigma\eta = \xi^3 + \xi^{-3}, \sigma^2\eta = \xi^2 + \xi^{-2}\}$, so by Artin the minimal polynomial is $(x - \eta)(x - \sigma\eta)(x - \sigma^2\eta)$, which we can expand out and find to $= x^3 + x^2 - 2x - 1$. An exercise is the following generalization: Artin's theorem implies that every intermediate subfield of $\mathbb{Q}(\xi_p)$ is generated by sums of powers of ξ_p.

What about $\frac{\mathbb{Z}}{3} \subset \mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q})$? $\frac{\mathbb{Z}}{3} = \langle \sigma^2 \rangle$; we average the orbit of the subgroup $\langle \sigma^2 \rangle$ on ξ, and get $\xi + \sigma^2\xi + \sigma^4\xi = \xi + \xi^2 + \xi^4 =: \epsilon$. Then by Artin, $\mathbb{Q}(\epsilon) = \mathbb{Q}(\xi_7)^{\frac{\mathbb{Z}}{3}}$, so $[\mathbb{Q}(\epsilon)|\mathbb{Q}] = 2$. Then $G\epsilon = \{\epsilon, \epsilon'\}$ where $\epsilon' = \sigma\xi + \sigma\xi^2 + \sigma\xi^4 = \xi^{-1} + \xi^{-2} + \xi^{-4}$. Then the minimal polynomial of ϵ over $\mathbb{Q}$ is $(x-\epsilon)(x-\epsilon') = x^2+x+2$, which we find because the coefficient of x is $\xi + \xi^2 + \cdots + \xi^6$ which must $= 1$, and then the constant term can be found by similar group-theoretic reasoning (though we can easily verify this result holds by simply expanding out). This is a quadratic equation with discriminant -7, so $\mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{-7})$, which suggests the following:

Proposition: for $p > 2$ a prime, the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\xi_p)$ is $\mathbb{Q}(\sqrt{\pm p})$, where the $\pm$ is $(-1)^{\frac{p-1}{2}}$. As a sketch of one method of proving this, let $G = (\frac{\mathbb{Z}}{p})^\times = \langle \sigma \rangle$; set $\alpha = \xi + \sigma^2\xi + \cdots + \sigma^{p-3}\xi$; this is fixed by $\langle \sigma^2 \rangle \subset G$, so $\mathbb{Q}(\alpha)$ is the quadratic extension of $\mathbb{Q}$; $G\alpha = \{\alpha, \sigma\alpha\}$ where $\sigma\alpha = \sigma\xi + \sigma^3\xi + \cdots + \sigma^{p-2}\xi$. An exercise: compute $\alpha \times \sigma\alpha$, and hence the minimal polynomial of α, $(x-\alpha)(x-\sigma\alpha) = x^2 + x + \alpha \times \sigma\alpha$, and hence the discriminant of this quadratic, to find the result. This method is due to Gauss, and the intricate sums nvolving powers of ξ that it is necessary to use in this exercise are called Gauss sums. They are "really there" [in that they are useful far beyond this proof], and behave "nicely" because μ, the set of roots of $x^n - 1$, is a group.

Now, a full proof by an alternative method: recall that if K is a field and $f \in K[x]$ a polynomial, L the splitting field of K, Δ the discriminant of f ($\sum_{i<j}(\alpha_i - \alpha_j)^2$ where the α_i are the roots of f in L), we have $K \subset K(\sqrt{\Delta}) \subset L$ with $[K(\sqrt{\delta}) : K] = 1$ or 2; it is 1 iff $\mathrm{Gal}(f) \subset A_n$, 2 iff $\mathrm{Gal}(f) \not\subset A_n$. We claim $\Delta(x^p - 1) = (-1)^{\frac{p-1}{2}} p^p$, which then implies the proposition, since $\sqrt{p^p} = p^{\frac{p-1}{2}} \sqrt{p} \notin \mathbb{Q}$, so $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\pm p}) \subset \mathbb{Q}(\xi_p)$. First, a lemma: let $f(x) = (x - \alpha_1)\ldots(x - \alpha_n)$, then $\Delta(f) \pm f'(\alpha_1)\ldots f'(\alpha_n)$: $f'(x) = \sum_{i=1}^n (x-\alpha_1)\ldots(x-\alpha_{i-1})(x-\alpha_{i+1})\ldots(x-\alpha_n)$, so $f'(\alpha_i) = (\alpha_i - \alpha_1)\ldots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\ldots(\alpha_i - \alpha_n)$, as all the other terms vanish. So $f'(\alpha_1)\ldots f'(\alpha_n) = \prod_{i \neq j}(\alpha_i - \alpha_j)$ which $= (-1)^{\frac{p(p-1)}{2}} \prod_{i<j}(\alpha_i - \alpha_j)^2$, as we have changed the sign of $\frac{p(p-1)}{2}$ terms in the product.

So if $f = x^p - 1, f' = px^{p-1}$ so $\Delta = \pm p^p \xi^{(1+2+\cdots+p-1)(p-1)}$, as the roots are $1, \xi, \ldots, \xi^{p-1}$; this $= \pm p^p$ either by careful explicit evaluation (which gives the sign explicitly), or by observing that $\Delta \in \mathbb{Z}$ so $\xi^N \in \mathbb{Z}$, so $\xi^N = \pm 1$.

Corollary: $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \not\subset A_p$.

Exercise: compute $\Delta(x^{p^m} - 1)$ explicitly, and $\Delta(x^n - 1)$, and hence the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\xi_n)$.

Example: $p = 17$, $\mathbb{Q}(\xi_{17})$; the Galois group is $(\frac{\mathbb{Z}}{17})^\times = \frac{\mathbb{Z}}{16}$ with subgroups $1 \leq \frac{\mathbb{Z}}{2} \leq \frac{\mathbb{Z}}{4} \leq \frac{\mathbb{Z}}{8} \leq \frac{\mathbb{Z}}{16}$, so the corresponding subfields are $\mathbb{Q}(\xi_{17}) \supset K_3 \supset K_2 \supset K_1 \supset \mathbb{Q}$; from above we have $K_1 = \mathbb{Q}(\sqrt{17})$. Clearly $[K_i : K_{i-1}] = 2$ so $K_i = K_{i-1}(\sqrt{k})$ for some $k \in K_{i-1}$. So every element of $\mathbb{Q}(\xi_{17})$ is a "constructible" (by ruler and compass) real. But $K_3 = \mathbb{Q}(\eta)$ where $\eta = \xi_{17} + \xi_{17}^{-1} = 2\cos\frac{2\pi}{17}$, so $\cos\frac{2\pi}{17}$ is constructible. So we can construct the regular 17-gon by ruler and compass.

Theorem (Gauss): a regular n-gon is constructible iff $n = 2^k p_1 \ldots p_r$ where the p_i are distinct Fermat primes (of which the only known are 3,5,17,257,65537): $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\cos\frac{2\pi}{n})] = 2$, so $\cos\frac{2\pi}{n}$ is constrictible iff $\mathbb{Q}(\xi_n)$ is a constructible field.

For the forward implication, if $\mathbb{Q}(\xi_n)$ is constructible, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \#(\frac{\mathbb{Z}}{n})^\times$ is a power of 2, then as an exercise the reader may show if $n = p_1^{e_1} \ldots p_r^{e_r}$ for the

p_i distinct primes, then $\#(\frac{\mathbb{Z}}{n})^\times = \phi(n) = \prod_i p_i^{e_i-1}(p_i-1)$, the "Euler ϕ function". So odd primes p can only occur once in n, otherwise $p_i \mid p^{e_i-1} \mid \#(\frac{\mathbb{Z}}{n})^\times$, so $n = 2^k p_1 \dots p_n$; then observe that if p is prime and $p-1 = 2^m$ then m must be a power of 2, as otherwise write $m = qr$ with $q > 1$ odd, and then $x^q + 1 = (x+1)(x^{q-1} - x^{q-2} + \cdots + 1)$, so putting $x = 2^r$ we have a factorization of $2^m + 1$, but we assumed this was prime, a contradiction.

For the converse, if n is of this form, then we have $\#(\frac{\mathbb{Z}}{n})^\times$ is a power of 2, and now by the structure theorem for finite abelian groups it must $= \frac{\mathbb{Z}}{2^{a_1}} \times \frac{\mathbb{Z}}{2^{a_r}}$ for some $a_1 \geq a_2 \geq \cdots \geq a_r$; then we need a chain of subgroups whose subquotients (i.e. the quotient of the two subgroups) have order 2, but this is immediate by induction on the order - we just need a subgroup H of index 2 in $\frac{\mathbb{Z}}{2^{a_1}}$, then $H \times \frac{\mathbb{Z}}{2^{a_2}} \times \cdots \times \frac{\mathbb{Z}}{2^{a_r}}$ is a subgroup of index 2 and we induct.

Exercise, as seen in the fourth example sheet: if $n = 2^{a_2}3^{a_3}5^{a_5}\dots$ then $(\frac{\mathbb{Z}}{n})^\times = \prod_{p>2:e_p>1}(\frac{\mathbb{Z}}{p^{e_p-1}} \times \frac{\mathbb{Z}}{p-1}) \times (\frac{\mathbb{Z}}{2^{e_2-2}} \times \frac{\mathbb{Z}}{2})$, with the last term only appearing if $e_2 \geq 1$, since $(\frac{\mathbb{Z}}{p^n})^\times = \frac{\mathbb{Z}}{p-1} \times \frac{\mathbb{Z}}{p^{n-1}}$ for $n \geq 1, p \neq 2$ and $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2^{n-2}}$ for $p = 2$, and $(\frac{\mathbb{Z}}{mn})^\times = (\frac{\mathbb{Z}}{m})^\times \times (\frac{\mathbb{Z}}{n})^\times$ if $(m,n) = 1$.

Corollary/exercise: every finite abelian group is a quotient of $(\frac{\mathbb{Z}}{n})^\times$ for some n; this follows from Dirichlet's theorem on arithmetic progressions of primes, which implies $\frac{\mathbb{Z}}{p-1}$ has lots of factors. So every abelian group occurs as a Galois group of an extension of $\mathbb{Q}$. But much more is true: recall we have $\mathbb{Q} \subset L \subset \mathbb{Q}(\xi_n) \Rightarrow \mathrm{Gal}(L/\mathbb{Q})$ is abelian. The converse of tihs is also true: if $L/\mathbb{Q}$ is an abelian extension, then there is an n such that $L \subset \mathbb{Q}(\xi_n)$. This is called the "Kronecker-Weber Theorem", a part of "abelian class field theory",one of the high points of early 20th century mathematics, and the GL_1 case of the "Lenglands Program", which remains an important research area even today.

Note that if F is finite then G is the Galois group of some extension, since $G \subset S_n$ for some n, by e.g. taking $n = \#G$ and letting G act on itself; then take $L = K(z_1, \dots, z_n)$ and L/L^G is an extension as required.

8 Kummer extensions

(These are extensions of the form $\mathbb{Q}(\sqrt[n]{\theta})$ for $\theta \neq 1$)

Proposition: let L be a splitting field for $x^n - \theta \in K[x]$ where $\mathrm{char}K \nmid n, \theta \neq 0$. Then L contains a primitive nth root of 1, ξ, so $K \subset K(\xi) \subset L$, and $\mathrm{Aut}(L/K(\xi)) = \frac{\mathbb{Z}}{d}$, a cyclic group, for some $d \mid n$. Moreover, $x^n - \theta$ is irreducible iff $d = n$: $\frac{d}{dx}(x^n - \theta) = nx^{n-1}$, so $\mathrm{char}K \nmid n \Rightarrow \gcd(nx^{n-1}, x^n - \theta) = 1$, as $\theta \neq 0$, i.e. $x^n - \theta$ has n distinct roots $\alpha_1, \dots, \alpha_n$ in L. But $(\frac{\alpha_i}{\alpha_j})^n = \frac{\alpha_i^n}{\alpha_j^n} = \frac{\theta}{\theta} = 1$, so $\frac{\alpha_1}{\alpha_1}, \frac{\alpha_2}{\alpha_1}, \dots, \frac{\alpha_n}{\alpha_1}$ are n distinct nth roots of unity, all in L, i.e. $\#\mu_n(L) = n$, so we have a primitive nth root ξ of 1 in L, and the roots α_i are $\alpha, \alpha\xi, \dots, \alpha\xi^{n-1}$ [for e.g. $\alpha = \alpha_1$], so $L = K(\xi, \alpha)$. Define a map $\chi : \mathrm{Aut}(L/K(\xi)) \to \frac{\mathbb{Z}}{n}$ by $\chi(\sigma) = j$ where $\sigma\alpha = \xi^j\alpha$; this is well defined, since for any $\sigma \in \mathrm{Aut}(L/K(\xi))$, $\sigma\alpha$ is a root of $x^n - \theta$ so must $= \xi^j\alpha$ for some j. Then if $\tau\alpha = \xi^k\alpha$ then $\sigma\tau(\alpha) = \sigma(\xi^k\alpha) = \xi^k\sigma\alpha$, since σ fixes $K(\xi)$, so $= \xi^k\xi^l\alpha = \xi^{k+l}\alpha$, so $\chi(\sigma\tau) = \chi(\sigma) + \chi(\tau)$ and χ is a group homomor (note it depends on our choice of ξ); as before, χ is injective. So $\mathrm{Aut}(L/K(\xi))$ is a subgroup of $\frac{\mathbb{Z}}{n}$, so must be $\frac{\mathbb{Z}}{d}$ for some $d \mid n$. Finally, $x^n - \theta$ is irreducible over $\mathbb{K}(\xi)$ iff $\mathrm{Aut}(L/K(\xi))$ has a single orbits on its roots, $\Leftrightarrow \#\mathrm{Aut} \geq n \Leftrightarrow \#\mathrm{Aut} = n \Leftrightarrow [L : K(\xi)] = n$ (writing Aut for $\mathrm{Aut}(L/K(\xi))$).

Example: $x^6 + 3 \in \mathbb{Q}[x]$ is irreducible by Eisenstein; $L = \mathbb{Q}(\sqrt[6]{-3}, \xi_6$; recall $\Phi_6 = x^2 - x + 1$ so $\xi_6 = \frac{1}{2}(1 + \sqrt{-3})$ so $\mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{-3})$; $x^6 + 3$ is not irreducible over $\mathbb{Q}(\sqrt{-3})$ since it $= (x^3 + \sqrt{-3})(x^3 - \sqrt{-3})$.

We have $K \subset K(\xi) \subset L = K(\xi, \alpha)$. Let $G = \mathrm{Gal}(L/K)$; we have $N \triangleleft G$ where $N = \mathrm{Gal}(L/K(\xi)), N \cong \frac{\mathbb{Z}}{d}$ with $d \mid n$; $\mathrm{Aut}(K(\xi)/K) = \frac{G}{N} \subset (\frac{\mathbb{Z}}{n})^\times$ abelian. But note taht G need not be abelian, as e.g. $S_3 = \mathrm{Gal}(X^3 - 2)$ is not.

Example: semidirect product $\frac{\mathbb{Z}}{p} \rtimes (\frac{\mathbb{Z}}{p})^\times$, which can be considered as the group of matricies $\begin{pmatrix} \mu & a \\ & 1 \end{pmatrix}$ for $\mu \in (\frac{\mathbb{Z}}{p})^\times, a \in \frac{\mathbb{Z}}{p}$ [I think this is meant to be an example of how a product of abelian groups may be nonabelian. By the end of this course, none of the students attending had any idea what the lecturer was going on about].

(Aside: semidirect products: suppose G is a group acting on another group N by group automorphisms; write g_n for $(\phi(g))(n)$. Then $G \times N$ forms a group $G \rtimes N$ [this sign may or may not be back-to-front; the lecturer used it either way around at various points, whilst assuring us only one orientation was correct] under multiplication $(g_1, n_1)(g_2, n_2)$ (informally, $= g_1 g_2 g_2^{-1} n_1 g_2 n_2 = g_1 g_2 g_{2n_1} n_2$) $= g_1 g_2, g_{2n_1}, n_2)$. For example, $(\frac{\mathbb{Z}}{p})^\times$ acts on $\frac{\mathbb{Z}}{p}$ by multiplication $a_b = ab$. Observe that if Γ is a group and $N \triangleleft \Gamma$ then Γ acts on N by conjugation. Semidirect products give us some of the groups of this form, but not all of them, since if $\Gamma = G \rtimes N$ then we have $N \triangleleft \Gamma$ and G a subgroup of Γ, So if $\frac{\Gamma}{N}$ is a subgroup of Γ, then it is a semidirect product. It is an exercise for the reader to find an explicit $N \triangleleft \Gamma$ such that $\frac{\Gamma}{N}$ is not a subgroup)

Corollary: Let $\theta \in K$, suppose $\mathrm{char}K \nmid n$, and K contains a (and therefore all) primitive nth root of unity. Let L be a splitting field for $x^n - \theta$. Then $\mathrm{Aut}(L/K)$ is cyclic, of order dividing n.

Amazingly, this corollary has a converse:

Theorem: let L/K be Galois with $\mathrm{Aut}(L/K) = \frac{\mathbb{Z}}{n}$ - "L/K is a cyclic extension". Suppose $\mathrm{char}K \nmid N$ and K contains a primitive nth root of unity. Then $\exists \theta \in K$ such that "$L = K(\sqrt[n]{\theta})$", i.e. $x^n - \theta$ is irreducible [over K] and L is a splitting field for it. This is an important theorem, though its proof is not hard: let $\mathrm{Aut}(L/K) = \langle \sigma \rangle = \{1, \sigma, \ldots, \sigma^{n-1}\}$. Consider L as a K-vector space; $\dim_K L = n$. $\sigma : L \to L$ is a K-vector space map; as $\sigma^n = 1$ we have all eigenvalues of σ are nth roots of 1 (and so the eigenvalues are in K), there is an eigenvalue of σ which is a primitive nth root (as otherwise σ has smaller order [than n]), and σ is diagonalisable, since as $\mathrm{char}K \nmid n$ it has n distinct eigenvalues. Let $\xi \in K$ be a primitive nth root of 1 which is an eigenvalue of σ and $\alpha \in L$ be acorresponding eigenvector: $\sigma\alpha = \xi\alpha$. Then $\alpha \notin K$ as $K = L^{\langle\sigma\rangle}$, but $\sigma(\alpha^n) = (\sigma\alpha)^n = (\xi\alpha)^n = \alpha^n$ so $\alpha^n \in K$; let it be θ. Then $x^n - \theta = (x - \alpha)(x - \xi\alpha)\ldots(x - \xi^{n-1}\alpha)$, as $(\xi^i\alpha)^n = \alpha^n = \theta$. So $x^n - \theta$ is an irreducible polynomial over K, as its roots form a single orbit under $\mathrm{Aut}(L/K) = \langle\sigma\rangle$, so the splitting field for $x^n - \theta$, $K(\alpha)$, has degree n, but it is contained in L and $[L : K] = n$, so $K(\alpha) = L$ and we have the result. Moreover, we can explicitly find α: the linear map $p_\xi : L \to L$ given by $p_\xi(x + \xi^{-1}\sigma x + \xi^{-2}\sigma^2 x + \cdots + \xi^{-(n-1)}\sigma^{n-1}x)$ (or, if the reader prefers, this divided by n, so that the map really is projection) has $p_\xi(L)$ non-zero and projects L onto $K\alpha$, the eigenspace of σ with eigenvalue ξ.

Example: cubics $f(x) = x^3 + px + q$ where $\mathrm{char}K \neq 2, 3$; $\Delta = -4p^3 - 27q^2, \delta = \sqrt{\Delta}$, L is the splitting field of f, $L = K(\alpha_1, \alpha_2, \alpha_3), f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

with $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Suppose $\xi_3 = \frac{1}{2}(1 + \sqrt{-3}) \in K$, i.e. $\sqrt{-3} \in K$, and $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in K$, and f is irreducible over K. Then, since $\delta \in K$, $\mathrm{Aut}(L/K) \subset A_3 = \frac{\mathbb{Z}}{3}$; since f is irreducible we have equality, so by the theorem, $L = K(\sqrt[3]{\theta})$ for some $\theta \in K$; this is a nonobvious result. So any element of L, in particular the roots of f, is a linear combination of $1, \sqrt[3]{\theta}, (\sqrt[3]{\theta})^2$, so we can "solve such a cubic by radicals"; we shall do this in a moment.

So any cubic (in char$K \neq 2, 3$) is solvable by radicals: we can write $f(x) = x^3 + px + q$ by completing the cube, put $K' = K(\sqrt{3}, \sqrt{\Delta})$, L' the splitting field of f over K' (i.e. the splitting field of $(x^3 - 1)(x^2 - \Delta)f(x)$ over K). If f is not irreducible over K' it factors as the product of a quadratic and a linear, and we can already solve quadratics by radicals so we can solve f. If f is irreducible we're in the situation above, so $\exists \theta \in K'$ such that $L' = K'(\sqrt[3]{\theta})$; such a θ is of the form $c_1 + c_2\sqrt{-3} + c_3\sqrt{\Delta} + c_4\sqrt{-3\Delta}$ for $c_i \in K$, so we can write all elements of L', and in particular the roots of f, as things involving sums of iterated nth roots - we can solve the cubic by radicals.

So, let's find the roots of f: set $\beta = p_{\xi^{-1}}(\alpha_1) = \alpha_1 + \xi\alpha_2 + \xi^2\alpha_3$, $\gamma = p_\xi(\alpha_1) = \alpha_1 + \xi^2\alpha_2 + \xi\alpha_3$. So $1, \beta, \gamma$ form a basis of L/K, each lying in the σ-eigenspace with respective eigenvalues $1, \xi^{-1}, \xi$; by the theorem $\beta^3, \gamma^3 \in K$; we would like to find them in terms of the coefficients of f. Then we will be done, since $\alpha_1 = \frac{1}{3}(\beta + \gamma), \alpha_2 = \frac{1}{3}(\xi^2\beta + \xi\gamma), \alpha_3 = \frac{1}{3}(\xi\beta + \xi^2\gamma)$.

Claim: 1) $\beta\gamma = -3p$ 2) β^3, γ^3 are the roots of $x^2 + 27qx - 27p^3$; given this, by 2) we have $\beta^3, \gamma^3 = \frac{1}{2}(-27q \pm 3\sqrt{-3\Delta})$, so put $\theta = \frac{1}{2}(-27q + 3\sqrt{-3\Delta})$, then $\beta = \sqrt[3]{\theta}, \gamma = \frac{\beta}{p}$.

We prove the claim by explicit computation: 1) $\beta\gamma = (\alpha_1 + \xi\alpha_2 + \xi^{-1}\alpha_3)(\alpha_1 + \xi^{-1}\alpha_2 + \xi\alpha_3) = \alpha_1^1 + \alpha_2^2 + \alpha_3^1 + (\xi + \xi^2)\sum \alpha_i\alpha_j = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3p = -3p$. 2) by 1), $\beta^3\gamma^3 = -27p^3$, so we have to compute $\beta^3 + \gamma^3$; we find it is $3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3$; then as $f(\alpha_i) = 0$, $\alpha_i^3 = -p\alpha_i + q$, so $\sum \alpha_i^3 = -p\sum \alpha_i + 3q = 3q$ and $\beta^3 + \gamma^3 = -27q$, so $(x - \beta^3)(x - \gamma^3) = x^2 + 27qx - 27p^3$ as required.

Definition: i) L/K is an extension by radicals if there is a chain $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ where each L_i is obtained from L_{i-1} by adjoining a single root of $x^n - \theta_i$ for some $\theta_i \in L_{i-1}$, ii) L/K is contained in an extension by radicals if we have an extension by radicals L'/K such that $K \subset L \subset L'$, i.e. if every element of L can be written as a sum of iterated nth roots.

Definition: $f \in K[x]$ is solvable by radicals if its splitting field is contained in an extension by radicals, e.g. any quadratic or cubic is solvable by radicals.

[Herafter] assume L/K is Galois with $G = \mathrm{Aut}(L/K)$

Lemma/Example: Suppose K contains a primitive $|G|$th root of unity and G is abelian; then L/K is an extension by radicals: we have $G \cong \frac{\mathbb{Z}}{n_1} \times \cdots \times \frac{\mathbb{Z}}{n_k}$, induct on $\#G$. Put $N = \frac{\mathbb{Z}}{n_1}$; we have $N \triangleleft G$ since G is abelian, so $K \subset K^N \subset L$, then $[L : L^N] = \frac{\mathbb{Z}}{n}$, so by the fundamental theorem of Galois theory L^N/K is Galois with Galois group $\frac{G}{N}$, but $\frac{G}{N}$ is abelian, $\cong \frac{\mathbb{Z}}{n_2} \times \cdots \times \frac{\mathbb{Z}}{n_k}$, so by the induction hypothesis L^N/K is an extension by radicals. Now L/L^N is a cyclic extension, ond K (and hence L^N) contains all nth roots of unity, so by Kummer theory $L = L^N(\sqrt[n_1]{\theta})$ for some $\theta \in L^N$ and we are done.

Corollary: If G is abelian, and K arbitrary with char$K \nmid \#G$, then L/K is contained in an extension by radicals: put $l = \#G$, and we have an extension

$L \supset K$, but then $L \subset L(\xi_l) \supset K(\xi_l) \supset K$, where $L(\xi_l$ is a splitting field for $x^l - 1$. We claim $\mathrm{Aut}(L(\xi_l)/K(\xi_l)) \hookrightarrow \mathrm{Aut}(L/K)$, i.e. is a subgroup of $\mathrm{Aut}(L/K)$: since L/K is Galois, L is the splitting field of some polynomial $f \in K[x]$, so $L(\xi_l)$ is the splitting field of this f regarded as a polynomial over $K(\xi_l)$. Now if $\sigma \in \mathrm{Aut}(L(\xi_l)/K(\xi_l))$ then σ preserves f, so permutes its roots, so $\sigma(L) \subset L$, so we have a map $\mathrm{Aut}(L(\xi_l)/K(\xi_l)) \to \mathrm{Aut}(L/K)$. This map is injective, as $\sigma = 1$ iff it fixes all the roots of f (so $\sigma \in \mathrm{Aut}(L(\xi_l)/K(\xi_l))$ fixes all the roots of $f \Leftrightarrow \sigma$ fixes all the roots of f over K, as all the roots are the same, $\Leftrightarrow \sigma : L \to L$ is the identity). So $K \subset K(\xi_l) \subset L(\xi_l)$ is an extension by radicals, by the above, so $L \subset L(\xi_l)$ is contained in an extension by radicals.

Example: If L is the splitting field of $x^n - \theta$, $K \subset K(\xi_n) \subset L$, $[L : K(\xi_n)] = N = \frac{\mathbb{Z}}{d} \subset \frac{\mathbb{Z}}{n}, [K(\xi_n) : K] = \frac{G}{N} = \frac{\mathbb{Z}}{k} \subset (\frac{\mathbb{Z}}{n})^\times$ $(k \mid \#(\frac{\mathbb{Z}}{n})^\times)$. Note that the above proof works for G not necessarily abelian, e.g. $x^3 - 2$ has $G = S_3$, but the above proof holds, so in fact we only need a weaker condition. We used the properties that 1) $\exists N \triangleleft G$ such that $\frac{G}{N}$ is cyclic, 2) N is one of the class of groups we can handle by this proof (this is what our earlier talk of being "built out of cyclic groups" referred to), and 3) if G is in this class and $H \leq G$, then H is also in this class. We therefore define the following, which clearly has the first two properties; we will need to prove the third.

Definition: G is solvable if there is a chain of subgroups $1 = G_0 \leq G_1 \leq \cdots \leq G_r = G$ such that i) each $G_i \triangleleft G_{i+1}$, ii) $\frac{G_{i+1}}{G_i}$ is a cyclic group. (exercise: equivalent to define by i) as given and ii'): $\frac{G_{i+1}}{G_i}$ is abelian).

Examples of solvable groups: i) abelian groups, ii) $(\frac{\mathbb{Z}}{n}) \rtimes (\frac{\mathbb{Z}}{n})^\times$ as defined above ($\frac{\mathbb{Z}}{n}$ is the normal subgroup and $(\frac{\mathbb{Z}}{n})^\times$ the quotient group). iii) (exercise) $B := \{\begin{pmatrix} a_1 & b_1 & \dots & \dots \\ 0 & \dots & \dots & \dots \\ \dots & \dots & \dots & b_{n-1} \\ \dots & \dots & 0 & a_n \end{pmatrix} \in GL_n(F_p)\}$, the group of upper-triangular invertible matricies over F_p (note the $n = 2$ case proves ii), since as mentioned above we can write the elements of $\frac{\mathbb{Z}}{n} \rtimes (\frac{\mathbb{Z}}{n})^\times$ as $\begin{pmatrix} a & b \\ & 1 \end{pmatrix}$ for $a \in (\frac{\mathbb{Z}}{n})^\times, b \in \frac{\mathbb{Z}}{n}$. iv) If G is simple then it is not solvable.

Proposition: i) If G is solvable and $G \leq G$ then H is solvable: if G is solvable we have a chain of subgroups $1 = G_0 \leq \cdots \leq G_r = G$; put $H_i = G_i \cap H$, then we have $1 = H_0 \leq H_1 \leq \cdots \leq H_r = H$. If $h \in H_{i+1}$ then $hG_ih^{-1} = G_i$ since $G_i \triangleleft G_{i+1}$, so $h(G_i \cap H)h^{-1} \subset G_i \cap H$, so $H_i \triangleleft H_{i+1}$ Then it is an exercise that $\frac{G_{i+1} \cap H}{G_i \cap H} \hookrightarrow \frac{G_{i+1}}{G_i}$ by $h(G_i \cap H) \mapsto hG_i$ is an (injective) group homomorphism, so $\frac{H_{i+1}}{H_i}$, ii) For G a group and $N \triangleleft G$, G is solvable iff N and $\frac{G}{N}$ are solvable - exercise.

Theorem (Galois, the night before he died, if that wasn't just the lecturer making a joke): Let $f \in K[x]$, $\mathrm{char}K = 0$ or $\mathrm{char}K > \deg f$. Let L be the splitting field of f. Then f is solvable by radicals iff $\mathrm{Gal}(L/K)$ is solvable.

Example: $x^5 + 2x + 6 \in \mathbb{Q}[x]$ has Galois group S_5 which isn't solvable, so isn't solvable by radicals.

We have prooved the reverse implication above; for the forward, assume f is solvable by radicals (then we need to show $\mathrm{Gal}(L/K)$ is a solvable group): we have a chain of field $K = K_0 \subset K_1 = K_0(\beta_1) \subset K_2 = K_1(\beta_2) \subset \cdots \subset K_r = K_{r-1}(\beta_r) = M$, where $\beta_i^{r_1} \in K_{i-1}$, and f splits completely in M, i.e. $L \subset M$. Let $N = \mathrm{lcm}\{r_i\}$; replace K_0 with $K(\xi_N)$ where ξ_N is a primitive Nth root of 1, and inductively replace K_i by $K_{i-1}(\beta_i)$; all our assumptions still hold.

Case 1: suppose M/K is Galois. We have $K \subset L \subset M$; it is enough to show that Aut(M/K is solvable, as then by the fundamental theorem of Galois theory L/K is Galois and Aut(L/K) is a quotient of Aut(M/K), and quotients of solvable groups are solvable. Set $G_i = \mathrm{Aut}(M/K_i)$; we have $\mathrm{Aut}(M/K) \supset G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$. As $\xi_N \in K_0$, for $i \geq 1$ $K_i = K_{i-1}(\beta_i) \supset K_{i-1}$ is a Galois extension, since it is a splitting field for $x^{n_i} - \beta^{n_i}$, and cyclic by Kummer theory: it has Galois group a subgroup of $\frac{\mathbb{Z}}{n_i}$. For $i = 0$, $K_0 = K(\xi_N)/K$ is Galois also. But now M/K is Galois, so MlK_i is Galois, but by the above K_{i+1}/K_i is Galois, so by the fundamental theorem of Galois theory, $G_i \lhd G_{i+1}$ and $\frac{G_{i+1}}{G_i}$ is a subgroup of $\frac{\mathbb{Z}}{n_i}$, so cyclic. So G is solvable.

Case 2: if M/K is not Galois, we can reduce to case 1 by the following proposition:

Proposition: Let M/K be an extension by radicals, then there is an extension N/M by radicals such that N/K is Galois.

We do really need to prove something here: consider $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}), M = \mathbb{Q}(\sqrt[4]{2} = \sqrt{\sqrt{2}})$; we have L/K and M/L quadratic so Galois, but M/K is not Galois, since if it were, it would have to be the splitting field of $x^4 - 2$, but it doesn't contain $i\sqrt[4]{2}$; informally, this happens because we didn't adjoin $\sqrt{-\sqrt{2}}$ to L to make M, but to make a Galois extension we need to do the same thing to all the roots in L/K, not just one of them. (For a more rigorous proof, we can find $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \frac{\mathbb{Z}}{2}$, but we clearly have $4 = [\mathbb{Q}(\sqrt[4]{2} : \mathbb{Q}] \neq \#\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$.

Lemma: For L/K Galois, $\theta \in L$, $K \subset L \subset L(\beta)$ where $\beta^n = \theta$, and $\xi_n \in K$, $\exists$ an extension $N/L(\beta)$ by radicals such that N/K is Galois. Given this, we have the proposition: inductively, we work up the chain. K_0/K is Galois; we apply the lemma to $K_1 = K_0(\beta)$, and optain N_1 such that N_1/K is Galois and an extension by radicals and $K_1 \subset N_1$. Then apply the lemma to $N_1(\beta_2)/N_1$, obtaining N_2 such that N_2/K is Galois and an extension by radicals and $K_2 \subset N_2$, and so on.

Proof of lemma: Let $G = \mathrm{Aut}(L/K)$, $h(x) = \prod_{\sigma \in G}(x^n - \sigma\theta) \in L[x]$. Then $h(x) \in L[x]^G$, which $= K[x]$ as L/K is Galois. Also, as L/K is Galois, it is the splitting field of some polynomial $f \in K[x]$. Let N be the splitting field of fh over K; then N/K is Galois. N is the splitting field of fh, and hence of h, over L, so N is obtained from L by adding, for each $\sigma \in G$, all the roots of $x^n - \sigma\theta$. So N is a radical extension of L, as we obtained it from L by adding 1) the primitive nth roots of 1 and 2) $\forall \sigma \in G$, a single root $\sqrt[n]{\sigma\theta}$.

9 Quartics

[Suppose] $f \in K[x]$, $\deg f = 4$. We want to find the roots of f and find its Galois group; by Kummer theory the second will give us the first. Let L be the splitting field [of f], assume char$K \geq 5$, then $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$ (over L), and by completing the fourth power we can wlog take $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, so $f(x) = x^4 + px^2 + qx + r$. Assume f is irreducible; the Galois group acts transitively on $\{\alpha_1, \ldots, \alpha_4\}$, so the possible Galois groups are $S_4, A_4, D_4 = \frac{\mathbb{Z}}{4} \rtimes \frac{\mathbb{Z}}{2} = \langle(1234), (12)(34)\rangle, \frac{\mathbb{Z}}{4} = \langle(1234)\rangle, V = \{1, (12)(34), (13)(24), (14)(23)\} \cong \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$ (there are three subgroups of S_4 isomorphic to $\frac{\mathbb{Z}}{4}$, but they are all conjugate; likewise for D_4. There are many subgroups $\cong \frac{\mathbb{Z}}{2}\times\frac{\mathbb{Z}}{2}$, but none of the others act transitively on $\{1, 2, 3, 4\}$. We have $V \triangleleft S_4$.

Now, how do we determine G, and hence solve f?

i) Let $\Delta = \mathrm{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2, \delta = \sqrt{\Delta}$. If $\delta \in K$, we have $G \subset A_4$ so G is one of V, A_4; if $\delta \notin K$, $G \not\subset A_4$ so G is one of $\frac{\mathbb{Z}}{4}, D_4, S_4$.

ii), G is solvable, $V \triangleleft S_4$, so $V \triangleleft A_4$; we have $1 \triangleleft V \triangleleft A_4 \triangleleft S_4$ with quotients $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}, \frac{\mathbb{Z}}{3}, \frac{\mathbb{Z}}{2}$ respectively. So S_4 is solvable. So we have $1 \leq G \cap V \leq G \cap A_4 \leq G$, where G may be V (in which case we have $1 \leq V \leq V \leq V$), A_4 ($1 \leq V \leq A_4 \leq A_4$), D_4 ($1 \leq V \leq V \leq D_4$), $\frac{\mathbb{Z}}{4}$ ($1 \leq \frac{\mathbb{Z}}{2} \leq \frac{\mathbb{Z}}{2} \leq \frac{\mathbb{Z}}{4}$), or S_4 ($1 \leq V \leq A_4 \leq S_4$). The corresponding fields are $L \supset M := L^{G\cap V} \supset L^{G\cap A_4} = K(\delta) \supset K$, so we need to study $M = L^{G\cap V}$. We Have $[L : M] = 1,2$ or 4 and $[M : K(\delta)] = 3$ or 1, as $\frac{G\cap A_4}{G\cap V}$ is a subquotient of $\frac{A_4}{V}$, so its quotient group is a subgroup of $\frac{\mathbb{Z}}{3}$ (for $H \leq G, G_1 \triangleleft G_2 \leq G, H\cap G_1 \triangleleft H\cap G_2$ we have an injection $\frac{G_2\cap H}{G_1\cap H} \to \frac{G_2}{G_1}$), $[K(\delta) : K] = 1$ or 2. So either $M/K(\delta)$ is a cubic extension, in which case $M = K(\delta)(\sqrt[3]{\sigma})$ for some $\theta \in K(\delta)$, or $M = K(\delta)$.

$L = K(\alpha_1, \dots, \alpha_4)$. Given any $\gamma \in L$, $\sum_{g\in G\cap V} g\gamma$ is $\in L^{V\cap G} = M$. We want to partially symmetrise polynomials in $\alpha_1, \dots, \alpha 4$ (remark for interest: we could do this universally, using the symmetric function theorem), e.g. $\alpha_1 \mapsto \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. $[L : M] \in 1, 2, 4$, so we should average quadratic (and possibly quartic) polynomials; a convenient choice of polynomials to aveage is $\beta = \alpha_1 + \alpha_2, \gamma = \alpha_1 + \alpha_3, \epsilon = \alpha_1 + \alpha_4$ (we have $\beta = -(\alpha_3 + \alpha_4)$ etc.). β, γ, ϵ span the same space as $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. $\beta^2 = (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$; recall $V = \{1, (12)(34), (13)(24), (14)(23)\}$, so $V\beta^2 = \beta^2$, i.e. $\beta^2 \in M$; similarly for γ^2, ϵ^2. Furthermore we have $G\beta^2$ [lecturer here put =, but must mean $\subset$] $\{\beta^2, \gamma^2, \epsilon^2\}$.

Claim: $L^{G\cap V} = K(\beta^2, \gamma^2, \epsilon^2)$; we clearly have $\supset$. To show equality, it is enough to show $\mathrm{Aut}(L/K(\beta^2, \gamma^2, \epsilon^2)) = G \cap V$, by Artin. So it suffices to show that $\beta^2, \gamma^2, \epsilon^2$ are distinct, as then $\{g \in S_4 \cap G : g\beta^2 = \beta^2, g\gamma^2 = \gamma^2, g\epsilon^2 = \epsilon^2\} = G \cap V$ (e.g. if $\gamma^2 \neq \epsilon$, we have $(12) \notin$ this set, as $(12)\gamma^2 = \epsilon^2$. [Lecturer became incomprehensible] (By orbit-stabiliser, the elemnts which fix $\{\beta^2, \gamma^2, \epsilon^2\}$ must be D_4). If $\beta^2 = \gamma^2$ then $\beta = \pm\gamma$, i.e. $\alpha_2 = \alpha_3$ or $2\alpha_1 + \alpha_2 + \alpha_3 = 0$, which implies $\alpha_1 = \alpha_4$. But the roots $\alpha_1, \dots, \alpha_4$ are distinct ($\mathrm{char} K > 3$, so the extension is separable).

Define $g(x) = (x - \beta^2)(x - \gamma^2)(x - \epsilon^2)$, the "resolvent cubic", which is $\in K[x]$ as G permutes its roots; as the roots are G-invariant, the coefficients are symmetric fuctions of $\alpha_1 \dots, \alpha_4$, so we can write $g(x)$ in terms of the coefficients p, q, r of f (in fact, as we can show by carefully expanding out, $g(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$), and as M is the splitting field of g/K and g is a cubic, which we can solve, we can find all the roots of f by radicals: we solve for $\beta^2, \gamma^2, \epsilon^2$ by solving cubics, take square roots to get β, γ, ϵ (choosing signs such that $\beta\gamma\epsilon = -q$ - we have a free choice of the signs of β, γ, but then must take $\epsilon = -\frac{q}{\beta\gamma}$), and then β, γ, ϵ were a basis, so we can find the roots: $\alpha_1 = \frac{1}{2}(\beta + \gamma + \epsilon), \alpha_2 = \frac{1}{2}(\beta - \gamma - \epsilon)$, etc.

But in the process wee have almost determined the Galois group: if g is reducible, then $M = K(\delta)$, i.e. G fixes at least one of $\beta^2, \gamma^2, \epsilon^2$, which is the case iff $G \cap V = G \cap A_4$ (since it means $\#\frac{G\cap A_4}{G\cap V} = 1$), which is the case iff G is one of $D_4, \frac{\mathbb{Z}}{4}, V$. So we have four cases: if Δ is a square (in K) and g reducible then the Galois group is V, if Δ is a square but g irreducible then the group is A_4, if Δ is not a square and g is reducible then the group is one of $D_4, \frac{\mathbb{Z}}{4}$, and if Δ is not a square and g is irreducible then the group is S_4. We can see this as having checked $[G : G \cap A_4]$ by Δ and $[G \cap A_4 : G \cap V]$ by g; together these distinguish all the possibilities except for the case where the group may by D_4 or $\frac{\mathbb{Z}}{4}$. We can continue this analysis, and find polynomials in p, q, r when g is reducible and δ not a square, which detect whether the group is D_4 or $\frac{\mathbb{Z}}{4}$.

A fun/silly application: for char$K \neq 2$, set $\alpha = \sqrt{r + s\sqrt{t}}$ for $r, s, t \in K$. When can this be written as $\sqrt{a} + \sqrt{b}$ for some $a, b \in K$? We have solved this: write down a quartic with α as a root, e.g. $f(x) = (x^2 - r - s\sqrt{t})(x^2 - r + s\sqrt{t}) = x^4 - 2rx^2 + (r^2 - s^2 t)$. Let L be the splitting field of f; since f was obtained by iterated square roots, $[L : K] \in 1, 2, 4, 8$. $L = K(\sqrt{a}, \sqrt{b})$ ("L is biquadratic") iff $G = \mathrm{Aut}(L/K)$ is $V = \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$. So If $|G| = 8$, we cannot write α in the form $\sqrt{a} + \sqrt{b}$ (i.e. if the group is D_4, we cannot do this); if $|G| = 4$, the case $\frac{\mathbb{Z}}{4}$ is not ok either. So L is biquadratic iff $\Delta = \mathrm{disc}(f)$ is a square (A_4 and S_4 are impossible, as they have orders other than 1,2,4,8). We know the roots of f are $\pm\alpha, \pm\sqrt{r - s\sqrt{t}}$, so we can easily calculate $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 = 2^8 s^4 t^2 (r^2 - s^2 t)$, which is a square iff $r^2 - s^2 t$ is a square in K.

10 Function Fields, and a dictionary

$\mathbb{C}[x]$ is the set of polynomial functions $\mathbb{C} \to \mathbb{C}$; $\mathbb{C}(x)$ is the fraction field therof, the set of rational functions $\mathbb{C} \setminus$ {a finite set of points} $\to \mathbb{C}$. Let $K = \mathbb{C}(x), L = K(\sqrt{x^3 - x}) = \frac{\mathbb{C}(x)[y]}{y^2 = x^3 - x}$. L/K is a Galois extension since it is quadratic; its Galois group $G = \langle\sigma\rangle$ where $\sigma y = -y, \sigma x = x$. We ask what is the "meaning" of L? L is the fraction field of $R = \frac{\mathbb{C}[x,y]}{y^2 = x^3 - x}$, so we first examine R. We claim it is the ring of polynomial functions on $E = \{(x, y \in \mathbb{C}^2 : y^2 = x^3 - x\}$: $\mathbb{C}[x, y]$ is the set of polynomial functions $\mathbb{C}^2 \to \mathbb{C}$, and the function $y^2 = x^3 - x$ vanishes on E by the definition of E, so is $\equiv 0$ on E, so all functions in the ideal $(y^2 = x^3 + x)$ vanish on E, so R is a well defined ring of functions on E, and the functions we get are defined by polynomials, and the rest of the claim is true by the definition of E. So L is the set of rational functions on $E\setminus$ some finite set of points; the finite set of points where $\gamma(x, y) = \frac{p(x,y)}{q(x,y)}$ is not defined is the set of $(x, y) \in E$ where $q(x, y) = 0$.

The field inclusion $K = \mathbb{C}(x) \hookrightarrow L$ comes from the ring inclusion $\mathbb{C}[x] \hookrightarrow R$, which corresponds to a map on spaces $p : E \to \mathbb{C}$ by $(x, y) \mapsto x$. For each x except $0, 1, -1$ we have two possible ys (so there are two preimages in $p^{-1}(x)$); the map $p : E \to \mathbb{C}$ is a 2:1 covering map, except at 3 points of E. $\frac{\mathbb{Z}}{2} = \langle\sigma\rangle$ acts on E by $\sigma(x, y) = (x, -y)$; $\langle\sigma\rangle$ permutes the two points in the fibre of [a general x]. $\frac{E}{\langle\sigma\rangle}$ = the set of orbits of $\frac{\mathbb{Z}}{2}$ on $E = \mathbb{C}$, so we have a covering space $E \setminus 3$ points $\to \mathbb{C} \setminus 3$ points with covering group $\frac{\mathbb{Z}}{2}$, and the Galois group G is the group of this covering.

We can use this to sketch E: we can consider E as two planes above the plane of $\mathbb{C}$; over a small disc not including 0,1,-1, the preimage in E is two disjoint discs each of which bijects with our disc in $\mathbb{C}$. But over 0,1,-1, what happens?

Around $x = 0$, if $|x| << 1$ then we have $x^3 - x = -x(1 - x^2) \approx -x$, so in a small disc around $x = 0$, the equation looks like $y^2 = x$ (the lecturer changing x to $-x$ for amusement). What does $y^2 = x$ look like? Consider the projections

$p : (x, y) \mapsto x, q : (x, y) \mapsto y$; q is a bijection, so $P = \{(x, y) : y^2 = x\}$ is isomorphic to $\mathbb{C}$. So the preimage of a small disc about 0 is a single disc. $y^2 = x$ looks like a single copy of $\mathbb{C}$, but "wrapped around itself twice"; if we have an arc $\gamma(t) = e^{it}$ for $t \in [0, \pi]$ then under $p : y \mapsto y^2$ this becomes a circle, and similarly for the same map for $t \in [\pi, 2\pi]$. So the inverse image of a circle in the x plane is a circle wrapped around twice; Kummer extensions $y^n = x$ are wrapped around n times.

What is $E = \{(x, y) \subset \mathbb{C} : y^2 = x^3 - x\}$? To visualise, we first sketche it over $\mathbb{R}$; whe get an ellipselike section through 0 and -1, and then a disjoint curve passing through 1 on which y tends towards $\pm\infty$ as $x \to \infty$ (we can verify this because $2f\frac{dy}{dx} = 3x^2 - 1$, so if $x \geq 1, y > 0$ we have $y' > 0$ so the curve keeps increasing, but for $y < 0$ $y' < 0$ so the curve keeps decreasing also.

Now in $\mathbb{C}^2$, let $\Gamma = \{(x, y) \in E : y \in \mathbb{R}, x \in [-1, 0] \cup [1, \infty)\} = p^-1([-1, 0] \cup [1, \infty))$. Then $E \setminus \Lambda$ disconnects into two pieces, each $= \mathbb{C} \setminus ([-1, 0] \cup [1, \infty))$ - if you pick a branch of $\sqrt{x^3 - x}$ and move around continuously, you never get to the other branch, as to do so you would have to circle around $0, 1$ or -1. So E is two copies of this cut plane, "glued together": to do this we round the cuts a little, then take two copies, turn one over, and glue them along the edges of the cut. This gives us a pair of planes which come together to meet in a donut-like hole and then at a similar hole stretched out to infinity - if we add the point at infinity, we just have two spheres each with a circle missing, and are gluing along these circles, thus making a torus. So E is a torus minus a single point.

So the solutions of algebraic equations have topologies; they are (interesting) topological spaces, and the Galois group is the covering group (group of deck transformations). A Galois extension corresponds to a covering map in topology. We have a dictionary: if X is a topological space, it corresponds $C(X)$ the ring of continuous functions $X \to \mathbb{C}$ under pointwise addition and multiplication; if X is an algebraic variety or complex manifold, this corresponds to the subring $O(X)$ of algebraic or holomorphic functions $X \to \mathbb{C}$, respectively. Then if $K(X)$ is the fraction field of $O(X)$, the union of the sets of functions defined on U over all open $U \subset X$ [I have no idea, really], $p \in X$ corresponds to a maximal ideal in $O(x)$, $m_p = \{f \in O(x) : f(p) = 0\}$; we have $\frac{O(x)}{m_p} = \mathbb{C}$.

An idea: any commutative ring can be thought of al the ring of functions on some topological space; points of this topological space correspond to maximal ideals of R, and algebraic properties of R translate into geometric properties of this topological space.

[Now the final, utterly incomprehensible lecture]

The Galois group is an avatar of the fundamental group $\pi_1(X)$. If X is a complex manifold/topological space/etc. we have $O(X)$ the ring of holomorphic/continuous/etc. functions $X \to \mathbb{C}$. Then a map $\pi : X \to Y$ of spaces corresponds to a ring homomorphism $O(Y) \to O(X)$ by $f \mapsto f \circ \pi$.

The reader may verify that if π is surjective then the map $O(Y) \to O(X)$ is injective; in this case it induces a map from $K(Y)$, the fraction field of $O(Y)$, to $K(X)$. Then $\pi^{-1}(y)$ is a finite set $\forall y \in Y$ iff $K(Y)/K(X)$ is an algebraic extension. If $K(Y)/K(X)$ is Galois, then there is a finite group G acting on X, freely on an open set $\mathring{X}$, and $\frac{\mathring{X}}{G} = \mathring{Y}$ is open in Y.

For $p \in X$, $\{f \in O(X) : f(p) = 0\}$ is a maximal ideal corresponding to the point p.

For number fields and function fields of Riemann surfaces (algebraic curves), we have finite extensions $K/\mathbb{Q}, K/\mathbb{C}(x)$ respectively. Functions defined everywhere on our curve then correspond to rings of integers in K:

Points on a curve correspond to maximal ideals, which correspond to prime ideals, so e.g. for the curve $\frac{\mathbb{C}[x,y]}{x^3-x=y^2}$ and number field $\mathbb{Q}(i)/\mathbb{Q}$, points $a \in \mathbb{C}$ with prime ideal $(x+a)\mathbb{C}[x]$ ($\frac{\mathbb{C}[x]}{(x-a)} = \mathbb{C}$), a corresponds to a prime p and so to $p\mathbb{Z}$, and thus to $\frac{\mathbb{Z}}{p\mathbb{Z}} = F_p$. Then an interesting question is: what is the analogue of a small disc on the curve? But first:

11 Reduction modulo p

If $f \in \mathbb{Z}[x]$, p prime, $f(x) = \sum a_i x^i$, let $\bar{f}(x) = \sum \bar{a}_i x^i \in F_p[x]$. We can study f by studying its reduction modulo p for various p, e.g. if $\bar{f}$ is irreducible then so is f. For another example, if $f(x) = x^4 + 5x^2 - 2x - 3$, consider this modulo 2; it is $x^4 + x + 1 = (x^2 + x + 1)^2$. Modulo 3, it is $x^4 - x^2 + x = x(x^3 - x + 1)$. So it must be irreducible over $\mathbb{Z}$, as if it had a factorization over $\mathbb{Z}$ then its factorizations modulo p would be refinements of this, which is impossible.

Theorem (without proof): if f is monic, $f \in \mathbb{Z}[x]$, p prime and $\bar{f}$ separable, then, considered as subgroups of S_n, $\mathrm{Gal}(f/\mathbb{Q}) \supset \mathrm{Gal}(\bar{f}/F_p)$. Corollary: if $\bar{f} = h_1 \dots h_r \in F_p[x]$ with the h_i irreducible of d_i, then $\mathrm{Gal}(f)$ contains an element of cycle type $(d_1, \dots, d_r)$ (i.e. a composition of disjoint cycles with these lengths); it is an exercise to deduce this from the theorem. Note that if $\bar{f}$ is separable then so is f, since $\Delta(\bar{f}) = \overline{\Delta(f)}$.

Going back to our consideration of a small disc: by the implicit function theorem we can take the centre to be 0 and have a single local coordinate x. Then functions become locally power series, elements of $\mathbb{C}[[x]]$. We can approximate these by cutting off f after n terms, getting elements of $\frac{\mathbb{C}[[x]]}{x^n} = \frac{\mathbb{C}[x]}{x^n}$.

Definition: $\mathbb{Z}_p$, the p-adic integers, is $\{(X_1, X_2, \dots) \in \frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p^2} \times \dots : x_i = x_{i+1} \mod p^i\}$ ("$\mathbb{Z}_p = \lim_{\leftarrow} \frac{\mathbb{Z}}{p^i\mathbb{Z}}$", an "inverse limit"). This is a ring under componentwise addition and multiplication. We can map $\mathbb{Z} \to \mathbb{Z}_p$ by $n \mapsto (n \mod p, n \mod p^2, \dots)$; this is an injective ring homomorphism.

Claim: if $n \in \mathbb{Z}$ with $p \nmid n$ then $\frac{1}{n} \in \mathbb{Z}_p$: since $p \nmid n$, $\gcd(p^i, n) = 1 \forall i$, so $\exists a_i, b_i$ such taht $a_i n + p^i b_i = 1$, i.e. a_i is, informally speaking, $\frac{1}{n} \mod p^i$. Then $\frac{1}{n} = (a_1, a_2, \dots)$.

So we have $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} : p \nmid n\} \hookrightarrow \mathbb{Z}_p$; note $p \mapsto (0, p, p, \dots)$, which does not have an inverse in $\mathbb{Z}_p$, since it is 0 modulo p (we have a ring homomorphism $\mathbb{Z}_p \to F_p$ by $(X_1, X_2, \dots) \mapsto X_1$). Exercise: $\mathbb{Z}_p$ is a PID, with unique prime ideal $p\mathbb{Z}_p$ (so $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} = F_p$).

Definition: $\mathbb{Q}_p = \mathrm{Frac}\mathbb{Z}_p$ (i.e. the fraction field of $\mathbb{Z}_p$), "p-adic numbers". This is $= \mathbb{Z}_p[\frac{1}{p}]$, so $\mathbb{Q} \subset \mathbb{Q}_p$.

An analogy: $\mathbb{Z}_p$ is like $\mathbb{C}[[x]]$, $\mathbb{Q}_p$ is like Laurent series $\mathbb{C}((x))$, $\overline{\mathbb{Q}_p}$ is like $\overline{\mathbb{C}((x))}$, which (exercise) $= \bigcup_{n \in \mathbb{Z}} \mathbb{C}((x^{\frac{1}{n}}))$; $[\overline{\mathbb{Q}_p} : \mathbb{Q}] = \infty$.

Proposition: $x^p - x \in \mathbb{Z}_p[x]$ factors completely in $\mathbb{Z}_p[x]$, i.e. $\mathbb{Z}_p$ contains all $(p-1)$st roots of unity. We need:

Lemma: if $a, b \in \mathbb{Z}$, $a \equiv b \mod p^n$ for som e$n \geq 1$, then $a^p = b^p \mod p^{n+1}$. Proof: $a = b + p^n r \Rightarrow a^p = b^p + pb^{p-1}p^n r = \binom{p}{2} b^{p-2} p^{2n} r^2 + \dots \Rightarrow a^p \equiv b^p \mod p^{n+1}$.

Now, proof of the proposition: $x^p - x$ factors into distinct linear factors in $F_p[x]$. We shall use the lemma to "lift" this to $\mathbb{Z}_p$: let $\bar{a} \in F_p, a_0 \in \mathbb{Z}$ any integer such that $a_0 \mod p = \bar{a}$. Put $a_1 = a_0^p$; $a_0^p \equiv a_0 \mod p$ by Fermat. Then by the lemma, $a_1^p = (a_0^p)^p \equiv a_0^p \mod p^2$, by the lemma this $= a_1 \mod p^2$. Put $a_2 = a_1^p = a_0^{p^2}$, then $a_2^p = (a_1^p)^p =\equiv a_1^p = a_2 \mod p^3$ by the Lemma, and so on. So set $\tau(\bar{a}) = (a_0, a_0^p, a_0^{p^2}, \dots)$, and we have that this is $\mathbb{Z}_p$, and also that $\tau(\bar{a})^p = \tau(\bar{a})$, and if $\bar{a} \neq \bar{b}$ then $\tau(\bar{a}) \neq \tau(\bar{b})$ (as they're different modulo p). So this gives p distinct solutions to $x^p = x \in \mathbb{Z}_p$ (and so, as should be clear anyway, any choice of a_0 gives the same result).

Corollary: $\tau : F_p^\times \to \mathbb{Z}_p$ is a group homomorphism; we have $\tau(a)\tau(b) = \tau(ab)$, but $\tau(a) + \tau(b) \neq \tau(a + b)$. The map is called the "Teichmuller lift".

Example: $\sqrt{-1} \in \frac{\mathbb{Z}}{5}$ is 2, so $\tau(\bar{2}) = (2, 2^5, 2^{125}, \dots) \equiv (2, 7, 57, \dots)$.

So we have $F_p^\times \to \mathbb{Z}_p^\times \hookrightarrow \mathbb{Q}_p \supset \mathbb{Q}$; $\tau(F_p^\times) = \{\gamma \in \mathbb{Q}_p : \gamma^{p-1} = 1\}$. But $\mathbb{Q} \subset \mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}_p}$, so we have identified the elements of $F_p^\times$ with the $(p-1)$st roots of 1 in $\mathbb{C}$, by picking an isomorphism $\overline{\mathbb{Q}_p} \to \mathbb{C}$. So this is the "true" reason those roots form a group, and the nonuniqueness of the group structure on them corresponds precisely to the non-canonicalicity of our choice of isomorphism from $\overline{\mathbb{Q}_p}$ to $\mathbb{C}$.