LECTURE MARCH 27: ILLUSTRATIONS OF GALOIS THEORY

1. Quadratic extensions

Theorem 1.1. *Let F be a field of characteristic not 2. Then any extension E/F of degree 2 is Galois. We have $E = F(\sqrt{a})$ for some $a \in F$ which is not a square in F.*

Proof. Let E/F be an extension of degree 2. Then if $\alpha \in E$ does not belong to F, we have $E = F(\alpha)$. This element has some minimal polynomial over F, say $x^2 + bx + c$. Therefore $\alpha^2 + b\alpha + c = 0$. Complete the square:

$$\alpha^2 + b\alpha + b^2/4 + c = b^2/4,$$

so that

$$(\alpha + b/2)^2 = b^2/4 - c.$$

If $\beta = \alpha + b/2$, then $E = F(\beta) = F(\sqrt{b^2 - 4c}) = F(\sqrt{d})$, where $d = \sqrt{b^2 - 4c}$. The F-conjugate of $\sqrt{d}$ is just $-\sqrt{d}$, so E/F is a splitting field. Since $2 \neq 0$ in F, so that means that $\sqrt{d} \neq -\sqrt{d}$, since otherwise $2\sqrt{d} = 0$. □

Example 1.2. *Classify all quadratic extensions of* $\mathbf{Q}$.

Any quadratic extension of $\mathbf{Q}$ has to be $\mathbf{Q}(\sqrt{p/q})$, where $p, q \in \mathbf{Z}$, $q \neq 0$, and p/q is not the square of any rational number. We have $\sqrt{p/q} = \sqrt{pq}/q$. So we restrict our attention to $\mathbf{Q}(\sqrt{m})$, where $m \in \mathbf{Z}$ is not a perfect square. I only care about the case where m is not divisible by any square (m is square-free). So the complete list of quadratic extensions is:

$$\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{6}), \mathbf{Q}(\sqrt{7}), \mathbf{Q}(\sqrt{10}), \ldots,$$

and also:

$$\mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{-2}), \mathbf{Q}(\sqrt{-3}), \mathbf{Q}(\sqrt{-5}), \ldots,$$

Remember our definition of a constructible number:

Definition 1.3. *An algebraic number $\alpha \in \mathbf{C}$ is* constructible *if $\mathbf{Q}(\alpha)$ sits atop a tower of field extensions of $\mathbf{Q}$, each a quadratic extension of the last.*

This was the same as saying that the point α in the complex plane is constructible using a compass and ruler (and also a unit measure). Note that if α is constructible, then $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ must be a power of 2.

Another way of saying this is that you can write down α as an expression with nested square root signs.

2. Cyclotomic extensions

The central question here is:

Example 2.1. *For $m \geqslant 3$, investigate the splitting field of $x^m - 1$ over $\mathbf{Q}$.*

Such fields (and their subfields) are called *cyclotomic*. The complex roots of $x^m - 1$ lie on the unit circle, dividing it into m equal parts. "Cyclotomic" means "circle-cutting".

Let us fix m and write $\zeta = e^{2\pi i/m}$. Then ζ is a root of $x^m - 1$. In fact all roots of $x^m - 1$ are

$$\left\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\right\}.$$

These form a finite group under multiplication, and in fact a cyclic group. Any generator of this group is called a *primitive mth root of 1*.

Example 2.2. *Thus i and $-i$ are primitive 4th roots of 1, but 1 and -1 are not.*

If ζ is a primitive mth root of unity, then the other primitive mth roots of unity are ζ^a, where $1 \leqslant a \leqslant m$ are those numbers with $\gcd(a, m) = 1$. Thus in total there are $\phi(m)$ primitive mth roots of 1.

Theorem 2.3. *Let ζ be a primitive mth root of 1. Then $\mathbf{Q}(\zeta)$ is the splitting field of $x^m - 1$.*

Proof. All the roots of $x^m - 1$ are powers of ζ, and these obviously belong to $\mathbf{Q}(\zeta)$. □

Since $\mathbf{Q}$ is perfect, $\mathbf{Q}(\zeta)/\mathbf{Q}$ is separable. It's also a splitting field, and therefore it's Galois. What is $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$?

Given an automorphism $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, let's consider $\sigma(\zeta)$. We have $\sigma(\zeta)^m = \sigma(\zeta^m) = \sigma(1) = 1$. Therefore $\sigma(\zeta)$ is another mth root of 1, and so we have

$$\sigma(\zeta) = \zeta^j,$$

for some $j = 0, 1, 2, \ldots, m-1$. Since ζ was primitive, so is $\sigma(\zeta)$, and therefore $\gcd(j, m) = 1$. Let's call this automorphism σ_j. Furthermore,

$$\sigma_j \sigma_{j'} = \sigma_{jj'},$$

where the product jj' is taken modulo m.

Recall the group $\mathbf{Z}_m^\times$ of units modulo m. We have just described a group homomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \to \mathbf{Z}_m^\times$.

Theorem 2.4. *There is an isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \to \mathbf{Z}_m^\times$. Thus $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(m)$.*

Proof. (Sketch.) First of all, $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \to \mathbf{Z}_m^\times$ sends σ_j to j; it is clearly injective. I'm going to prove surjectivity in the case that $m = p$ is a prime number.

In that case $\phi(p) = p - 1$. It's enough to show that the degree $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p - 1$. The element ζ is a root of $x^p - 1$, but not of $x - 1$, so it is a root of

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

This polynomial is irreducible, you can apply the Eisenstein criterion at the prime p to this polynomial after shifting x to $x + 1$. □

Question: if m is not a prime number, what is the minimal polynomial of ζ over $\mathbf{Q}$? It must be some polynomial of degree $\phi(m)$, called the *cyclotomic polynomial*. The mth cyclotomic polynomial takes this form:

$$\Phi_m(x) = \prod_a (x - \zeta^a),$$

where a ranges over integers between 1 and m, relatively prime with m. It has integer coefficients!

For instance,

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

3. Constructibility of the 5-gon

Consider the extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ in the case $m = 5$. We have $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{Z}_5^\times = \{1, 2, 3, 4\}$. This is a cyclic group with generators 2 and 3.

What are all the subfields of $\mathbf{Q}(\zeta)$? By the main theorem of Galois theory, subfields of $\mathbf{Q}(\zeta)$ are in correspondence with subgroups of $\mathbf{Z}_5^\times$. There is one proper nontrivial subgroup, namely $\{1, 4\}$. Which is the subfield corresponding to this? We're looking for elements of $\mathbf{Q}(\zeta)$ which are fixed under the automorphism $\zeta \mapsto \zeta^4$.

Let

$$\tau = \zeta + \zeta^4 = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos(2\pi/5),$$

then τ lies in the subfield K fixed by σ_4. (By the way, σ_4 is complex conjugation. Thus τ is a real number.)

We know that $K/\mathbf{Q}$ is a quadratic extension. So it must be $K = \mathbf{Q}(\sqrt{m})$ for some integer m. Let's square τ:

$$\tau^2 = \zeta^2 + 2 + \zeta^3.$$

Now add τ to τ^2:

$$\begin{aligned} \tau^2 + \tau &= \zeta + \zeta^2 + \zeta^3 + \zeta^4 + 2 \\ &= (1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4) + 1 \\ &= 1 \end{aligned}$$

We have $\tau^2 + \tau - 1 = 0$, so that

$$\tau = \frac{-1 + \sqrt{5}}{2}$$

(we can reject the minus sign since $\tau > 0$.)

Let's go all the way and given an explicit formula for ζ. We have $\zeta + \zeta^{-1} = \tau$, so that $\zeta^2 - \tau\zeta + 1 = 0$ You can now come up with a formula for ζ:

$$\zeta = \frac{1}{2}(\tau + \sqrt{\tau^2 - 4}) = \frac{1}{2}\left(\frac{1}{2}(-1 + \sqrt{5}) + \sqrt{\frac{-5 - \sqrt{5}}{2}}\right)$$

4. Fermat primes

Gauss discovered which regular polygons were constructible. For instance he noted that

$$\begin{aligned} 16\cos\frac{2\pi}{17} &= -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \\ &\quad +2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}, \end{aligned}$$

and therefore that the regular 17-gon is constructible. What's the pattern?

Let's first handle the case of a regular p-gon, where p is a prime number. Let $\zeta = e^{2\pi i/p}$ be a pth root of 1. If ζ is constructible, it implies that $[\mathbf{Q}(\zeta) : \mathbf{Q}]$ is a power of 2: $p - 1 = 2^n$. Primes of the form $2^n + 1$ are called Fermat primes.

Since 7 is not a Fermat prime, the regular 7-gon is not constructible.

If $p = 2^n + 1$ is a Fermat prime, then $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{Z}_p^\times$. This is a cyclic group of order $p - 1 = 2^n$. This group contains one subgroup for each power of 2 between 1 and 2^n. By the main theorem of Galois theory, there exist fields

$$\mathbf{Q}(\zeta)/K_{n-1}/K_{n-2}/\cdots/K_1/\mathbf{Q},$$

where each field is quadratic over the next. Therefore ζ is constructible.

Cool exercise: if $p = 2^n + 1$ is a Fermat prime, then n itself is a power of 2.

So which numbers $2^{2^n} + 1$ are prime? First few: $3, 5, 17, 257, 65537$. It is unknown whether there are any others!

5. The hard midterm problems

Example 5.1. *Let F be a field of characteristic not 2 or 3, and suppose that $a \in F^\times$ is not a perfect cube in F. (a) Show that $f(x) = x^3 - a$ is irreducible in F. (b) Let E be the splitting field of $f(x)$. Carefully show that if -3 is a square in F, then $[E : F] = 3$, and otherwise, $[E : F] = 6$.*

Proof. (a) If a cubic polynomial factors, then it must have a root, but that would contradict the fact that a is not a cube in F.

(b) Suppose that -3 is a square in F, so that we can talk about an element $\sqrt{-3} \in F$. Since F does not have characteristic 2, it makes sense to write

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Then ω is a root of $x^2 + x + 1$ and hence of $x^3 - 1$. Furthermore we have $\omega \neq 1$, since otherwise $\sqrt{-3} = 3$ and then $-3 = 9$ or $12 = 0$ impossible since F does not have characteristic 2 or 3. Thus ω is a primitive 3rd root of 1: we have $\omega^3 = 1$, but $\omega \neq 1$.

Now let $r \in E$ be a root of $x^3 - a$. Then ωr and $\omega^2 r$ are also roots of $x^3 - a$, and they lie in $F(r)$. Therefore $E = F(r)$ is already the splitting field of $x^3 - a$; it has degree 3.

Conversely, suppose -3 is not a square in F. The polynomial $x^3 - a$ is separable over F (because F has characteristic not 3); let r_1, r_2, r_3 be the three distinct roots of $x^3 - a$ in E. Let $\omega = r_2/r_1$, so that $\omega \neq 1$. We have $\omega^3 = r_2^3/r_1^3 = a/a = 1$, so that ω is a root of

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

So $\omega^2 + \omega + 1 = 0$, and therefore

$$(2\omega + 1)^2 = 4\omega^2 + 4\omega + 1 = 4(\omega^2 + \omega + 1) - 3 = -3,$$

which means that $\sqrt{-3} \in E$. On the other hand, $\sqrt{-3} \notin F$, so it must have degree 2 over F, and therefore $[E : F]$ is divisible by 2. It is also divisible by 3 (since $F(r_1) \subset E$), so therefore it is divisible by 6. Since we know $[E : F] \leqslant 3! = 6$, we must have $[E : F] = 6$. □

Example 5.2. *Let F be a field of characteristic not 2 or 3, and let $f(x) = x^3 + px + q$ be an irreducible cubic polynomial with coefficients in F. Let r_1, r_2, r_3 be the roots of $f(x)$ in an algebraic closure of F. It can be shown that the element*

$$D = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$$

belongs to F. In fact it is equal to $-4p^3 - 27q^2$. Let $E = F(r_1, r_2, r_3)$ be the splitting field of $f(x)$. Show that if D is a square in F, then $[E : F] = 3$, and that if D is not a square in F, then $[E : F] = 6$.

The computational way. We have a tower of fields

$$E/F(r_1)/F,$$

where $E = F(r_1, r_2, r_3)$. We claim that

$$E = F(r_1, \sqrt{D}).$$

Let's see how this solves the problem. If $\sqrt{D} \in F$, then immediately we get $E = F(r_1)$, which has degree 3 over F. If $\sqrt{D} \notin F$, then $[F(\sqrt{D}) : F] = 2$, and since this $F(\sqrt{D}) \subset E$, we have $[E : F] = 6$ by the same reasoning as the last proof.

We have

$$x^3 + px + q = (x - r_1)(x - r_2)(x - r_3),$$

so that

$$\begin{aligned} r_1 + r_2 + r_3 &= 0, \\ r_1 r_2 r_3 &= -q \end{aligned}$$

Therefore

$$(x - r_2)(x - r_3) = x^2 + r_1 x - \frac{q}{r_1}.$$

Then

$$\sqrt{D} = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3) = (2r_1^2 - \frac{q}{r_1})(r_2 - r_3)$$

We get that $r_2 - r_3 \in F(r_1, \sqrt{D})$. But also $r_2 + r_3 = -r_1 \in F(r_1) \subset F(r_1, \sqrt{D})$. Therefore the sum and difference of these two elements, namely $2r_2, 2r_3$, also lies in $F(r_1, \sqrt{D})$. Since $2 \neq 0$ in F, we can conclude that $r_2, r_3 \in F(r_1, \sqrt{D})$. We have shown that $E = F(r_1, r_2, r_3) = F(r_1, \sqrt{D})$, which is what we needed for the proof. □

The better way, using Galois theory. Let $G = \mathrm{Gal}(E/F)$. Then G permutes the three roots r_1, r_2, r_3. Therefore we can think of it as a subgroup of S_3: $G \subset S_3$.

Think of what an element of G does to the discriminant:

$$D = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2.$$

It's pretty clear that permuting the roots doesn't change D! Therefore $D \in F$. Now let's examine what an element of G does to

$$\sqrt{D} = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3).$$

Let τ be a transposition (say, (12)). Then $\tau\sqrt{D} = -\sqrt{D}$. Let σ be a 3-cycle (say (123)). Then $\sigma\sqrt{D} = \sqrt{D}$.

Suppose $\sqrt{D} \in F$. Then $\sqrt{D}$ is fixed by all elements of G. Then G must not contain any transpositions. We conclude that $G = A_3 \cong \mathbf{Z}_3$. Whereas if $\sqrt{D} \notin F$, then there must be a transposition in G. We already know that $\#G$ is divisible by 3; therefore $G = S_3$. □

6. A coda on cyclotomic fields

If $m \geqslant 3$, we let

$$\zeta_m = e^{2\pi i/m}$$

be a primitive mth root of 1. The field $Q(\zeta_m)$ is called a cyclotomic field. We have seen that $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ is isomorphic to $\mathbf{Z}_m^\times$.

Let's assume that $m = p$ is an odd prime. Then $\mathbf{Z}_p^\times$ is a cyclic group of order $p - 1$. The main theorem of Galois theory says that subfields of $\mathbf{Q}(\zeta_p)$ are in bijection with subgroups of $\mathbf{Z}_p^\times$. In turn, subgroups of $\mathbf{Z}_p^\times$ are in correspondence with divisors of $p - 1$.

In particular, since $2|p - 1$, there exists a unique quadratic extension of $\mathbf{Q}$, call it K, contained in $\mathbf{Q}(\zeta_p)$. We have $K = \mathbf{Q}(\sqrt{m})$, where m is a squarefree integer.

Theorem 6.1 (Gauss, 1798, 21 years old)**.** *$m = p$ if $p \equiv 1 \pmod 4$, and $m = -p$ if $p \equiv 3 \pmod 4$.*

As an example, if $p = 5$, the theorem says that $\sqrt{5} \in \mathbf{Q}(\zeta_5)$. Actually, we knew this already, since

$$\zeta_5 + \zeta_5^4 = \frac{-1 + \sqrt{5}}{2}.$$

We can even rewrite this as

$$\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}.$$

The unique subgroup $H \subset \mathbf{Z}_p^\times$ of index 2 is the subgroup of squares modulo p. For instance, if $p = 5$, the subgroup H is $\{1, 4\} \subset \{1, 2, 3, 4\}$. Gauss designed an element of $\mathbf{Q}(\zeta_p)$ to be fixed under H.

To write it down, we need the *Legendre symbol*. For an integer a not divisible by p, we let

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

Gauss' theorem is then:

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a = \begin{cases} \sqrt{p} & p \equiv 1 \pmod 4, \\ \sqrt{-p} & p \equiv -1 \pmod 4 \end{cases}$$

We know that $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ is an abelian group, namely $\mathbf{Z}_m^\times$. Since every subgroup of an abelian group is normal, we have that every $K \subset \mathbf{Q}(\zeta_m)$ has to be Galois over $\mathbf{Q}$. Furthermore, $\mathrm{Gal}(K/\mathbf{Q})$ has to be abelian, since it is a factor group of $\mathbf{Z}_m^\times$.

Definition 6.2. *E/F is an* abelian extension *of fields if it is Galois and if* $\mathrm{Gal}(E/F)$ *is abelian.*

Theorem 6.3 (Kronecker-Weber theorem)**.** *Let $K/\mathbf{Q}$ be an abelian extension. Then K is contained in $\mathbf{Q}(\zeta_m)$ for some m.*

(Complete proof given by Hilbert in 1896. This might be considered the first result in *class field theory.*)

7. Symmetric functions

Let $n \geqslant 1$ be an integer, and let K be a field. Let

$$E = K(r_1, r_2, \ldots, r_n)$$

be the field generated over K by n indeterminates. The group S_n acts on E, by permuting the r_is. Thus $S_n \subset \mathrm{Aut}(E/K)$.

Let

$$F = E^{S_n}.$$

This is the field of *symmetric functions* in the $r_1, \ldots, r_n$. Thus, elements of F are rational functions in the $r_1, \ldots, r_n$ which are symmetric in those variables. For instance, the elements $r_1^2 + \cdots + r_n^2 \in F$ and $r_1 \cdots r_n$ belong to F.

Here's a way to cook up a bunch of elements of F. Let

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n).$$

A priori, this lies in $E[x]$. But since any permutation of the r_i doesn't change $f(x)$, all of the coefficients of $f(x)$ must be symmetric. Let's give names to those coefficients, by putting

$$f(x) = x^n - s_1 x^{n-1} + \cdots \pm s_{n-1} x \mp s_n$$

(the signs alternate). Then

$$\begin{aligned} s_1 &= r_1 + r_2 + \cdots + r_n \\ s_2 &= r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n \\ &\vdots \\ s_n &= r_1 r_2 \cdots r_n \end{aligned}$$

all belong to F. They are called the *elementary symmetric polynomials* in $r_1, \ldots, r_n$.

Theorem 7.1. *We have $F = K(s_1, \ldots, s_n)$. Thus, every symmetric function in $r_1, \ldots, r_n$ is a rational function in the elementary symmetric polynomials $s_1, \ldots, s_n$. The extension E/F is Galois, and* $\mathrm{Gal}(E/F) = S_n$.

Proof. For now we let $L = K(s_1, \ldots, s_n)$, so that we have a tower of fields:

$$\begin{array}{c} E = K(r_1, \ldots, r_n) \\ | \\ F = E^{S_n} \\ | \\ L = K(s_1, \ldots, s_n) \end{array}$$

The polynomial $f(x)$ lies in $L[x]$, and its splitting field is $L(r_1, \ldots, r_n) = E$. The roots are distinct, so that E/L is separable. Thus E/L is Galois. Since E/L is the splitting field of a polynomial of degree n, we have the inequality $[E : L] \leqslant n!$. But also, S_n is a subgroup of $\mathrm{Gal}(E/L)$, so that $[E : L] \geqslant n!$. Thus we have $[E : L] = n!$, and therefore $\mathrm{Gal}(E/L) = S_n$. By the main theorem of Galois theory, the fixed field of S_n is just L, so that $L = E^{S_n} = F$. □

For example, let $n = 2$, so that $F = K(s_1, s_2)$ and $E = K(r_1, r_2)$, with

$$\begin{aligned} s_1 &= r_1 + r_2 \\ s_0 &= r_1 r_2. \end{aligned}$$

The theorem states that any element of E which is unchanged by swapping r_1 and r_2 must be an element of F. For instance

$$r_1^2 + r_2^2 = s_1^2 - 2s_0.$$

Theorem 7.2. *Let G be any finite group. Then $G \cong \mathrm{Gal}(E/F)$, for some field extension E/F.*

Proof. There exists an n such that G is isomorphic to a subgroup of S_n (Cayley's theorem). We just saw that S_n is a Galois group, and therefore by the main theorem of Galois theory, so is G. □

Question: Given a finite group G, does there exist an extension $K/\mathbf{Q}$ such that $\mathrm{Gal}(K/\mathbf{Q}) \cong G$? This is called the *inverse Galois problem*, and it is wide open. It is known however for finite abelian groups, and also for S_n.