LECTURE APRIL 10: SOLVING POLYNOMIAL EQUATIONS BY RADICALS

1. Quadratic, cubic, quartic formulas

We start with the familiar quadratic formula. For rational numbers $b, c \in \mathbf{Q}$, the roots of

$$x^2 + bx + c$$

are

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

There is also a cubic formula (Cardano, 1545). We start with

$$x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbf{Q}$. We can get rid of the coefficients of x^2 by a subsitution $x \mapsto x - a/3$, to get a cubic in "depressed" form

$$x^3 + px + q.$$

The discriminant of this polynomial is $D = -4p^3 - 27q^2$. If $D > 0$, there are three real roots, and if $D < 0$, there is one real root and one complex-conjugate pair. The Renaissance Italians didn't really appreciate complex numbers, but it turns out that solving the cubic required them to deal with them. If $D < 0$, the one real root is

$$\sqrt[3]{-\frac{q}{2} + \frac{1}{6}\sqrt{\frac{-D}{3}}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{6}\sqrt{\frac{-D}{3}}}.$$

This was satisfactory, since you never have to take a square root of a negative number. But what if $D > 0$? Then there are three real roots. The above expression is one of them, but to obtain it, it's required to not only take a square root of a negative number, but then to take the cube root of a complex number – this involves trisecting an angle! The other two roots are

$$\omega\sqrt[3]{-\frac{q}{2} + \frac{1}{6}\sqrt{\frac{-D}{3}}} + \omega^2\sqrt[3]{-\frac{q}{2} - \frac{1}{6}\sqrt{\frac{-D}{3}}}$$

and

$$\omega^2\sqrt[3]{-\frac{q}{2} + \frac{1}{6}\sqrt{\frac{-D}{3}}} + \omega\sqrt[3]{-\frac{q}{2} - \frac{1}{6}\sqrt{\frac{-D}{3}}}$$

where ω is a primitive 3rd root of 1.

Just to reiterate, all this was necessary to find the *real* roots of a cubic polynomial, which has three real roots. One example is the polynomial

$$x^3 - \frac{3}{4}x + \frac{1}{8},$$

whose roots are $\cos(2\pi/9), \cos(4\pi/9), \cos(8\pi/9)$. In this case $D = 81/64$. The cubic formula is just going to tell you that

$$\cos(2\pi/9) = \frac{1}{2}(\sqrt[3]{\omega} + \sqrt[3]{\omega^2}).$$

This is a little unhelpful: we already knew the connection between trig functions and complex numbers.

Ferraro (1540) found a quartic formula, which allows one to find the roots of a polynomial of degree 4, but it has similar subtleties.

2. Radical extensions

Definition 2.1. *Let E/F be an algebraic extension of fields. We say E/F is* radical *if $E = F(z)$, where $z^n \in F$ for some $n \geqslant 1$.*

In other words, a radical extension is of the form $F(\sqrt[n]{\alpha})/F$ for some $\alpha \in F$.

As an example $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is a radical extension. As is $\mathbf{Q}(\zeta_m)$ for any $m \geqslant 1$.

Theorem 2.2. *Let F be a field of characteristic not 2. Let E/F be an extension of degree 2. Then E/F is radical.*

Proof. Use the quadratic formula! □

Example 2.3. *Let $F = \mathbf{Z}_2$, and let E/F be the splitting field of $x^2 + x + 1$. Is this a radical extension?*

We have $E = F(\alpha)$, where $\alpha^2 + \alpha + 1 = 0$. In fact $\alpha^3 = 1$. Thus E/F is radical.

Example 2.4. *Let $F = \mathbf{Z}_2(t)$. Let E be the splitting field of $x^2 - x - t$. Then $E = F(\alpha)$, where $\alpha^2 = \alpha + t$. Then E/F is not radical.*

Definition 2.5. *Let E/F be an algebraic extension. We say that E/F is* solvable *if E is contained in a field K/F, where K is the top of a tower of fields,*

$$K \supset K_1 \supset K_2 \supset \cdots \supset K_n \supset F,$$

where each field in the tower is radical over the one below it.

Thus elements of K (and thus E) are expressible using the field operations, elements of F, and nested radicals.

For instance, in characteristic not equal to 2, every degree 2 extension is solvable (in fact radical).

Cardano's formula says: Let F be a field of characteristic 0, and let $f(x)$ be a cubic polynomial in $F[x]$. Let E/F be the splitting field of $f(x)$. Then E/F is solvable.

The same is true for polynomials of degree 4.

Definition 2.6. *A polynomial $f(x) \in F[x]$ is* solvable *if its splitting field is a solvable extension of F.*

The big theorem here is that polynomials of degree 5 are not generally solvable. Some polynomials of degree 5 are solvable, such as $x^5 - 2$. The main point here is that some are not, for example $x^5 + x + 1$.

This theorem will involve some Galois theory. Let's start with a field F of characteristic 0, and an integer $n \geqslant 2$. Consider the extension $E = F(\sqrt[n]{\alpha})$, so that E/F is a radical extension. (Assume $\alpha \neq 0$.) Assume that F contains all roots of the polynomial $x^n - 1$ (all nth roots of 1). This polynomial has distinct factors (why??), let's call them $1, z, z^2, \ldots, z^{n-1} \in F$.

Let $\beta = \sqrt[n]{\alpha}$, so that $\beta^n = \alpha$. If β' is an F-conjugate of β, then $(\beta')^n = \alpha$ as well. Then

$$(\beta'/\beta)^n = \alpha^n/\alpha^n = 1,$$

so that $\beta'/\beta = z^i$ for some i. Since $z \in F$ by hypothesis, we have $\beta' = z^i\beta \in F(\beta) = E$. Thus E/F is a splitting field, hence Galois (remember we're in characteristic 0 so separability is automatic).

I don't know what $\mathrm{Gal}(E/F)$ is exactly, but I can say that there is a map

$$\mathrm{Gal}(E/F) \to \mathbf{Z}_n,$$

which goes like this. Given $\sigma \in \mathrm{Gal}(E/F)$, we must have $\sigma(\beta) = z^i\beta$ for some unique $i \in \mathbf{Z}_n$. In this map we send σ to i. Easy to see that this map is injective. If σ maps to i, let's call it σ_i. I claim this map is a homomorphism. We have

$$\sigma_i\sigma_j(\beta) = \sigma_i(z^j\beta) = z^j\sigma_i(\beta) = z^j z^i\beta = z^{i+j}\beta = \sigma_{i+j}(\beta)$$

Thus $\sigma_i\sigma_j = \sigma_{i+j}$, and thus this is an injective homomorphism. Thus we can think of $\mathrm{Gal}(E/F)$ as a subgroup of $\mathbf{Z}_n$. Therefore it is cyclic.

Let's now lift the assumption that F contains all roots of $x^n - 1$. Let E/F be the splitting field of $x^n - \alpha$. The roots of this are once again $z^i\beta$, for $i = 0, \ldots, n-1$. We have a tower $E/F(z)/F$. The previous argument shows that $\mathrm{Gal}(E/F(z))$ is a cyclic group. We also have the cyclotomic extension $F(z)/F$, which is also abelian: $\mathrm{Gal}(F(z)/F)$ is a subgroup of $\mathbf{Z}_n^\times$.

Both extensions are radical. We also see that if $G = \mathrm{Gal}(E/F)$. Then G contains a subgroup $H = \mathrm{Gal}(E/F(z))$, such that H is cyclic. We know that $F(z)/F$ is Galois, and therefore by the main theorem of Galois theory, H is a normal subgroup of G, and

$$G/H \cong \mathrm{Gal}(F(z)/F)$$

is an abelian group.

To review: the splitting field of $x^n - \alpha$ over F is Galois with group G. We have a normal subgroup $H \subset G$, such that both H and G/H are abelian. This is a very strong restriction on what G can be!

3. Solvable groups

The following definition was inspired by the question of solving polynomial equations in radicals.

Definition 3.1. *Let G be a group. We say that G is* solvable *if there exists a composition series*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G,$$

such that each G_i is normal in G_{i+1}, and such that G_{i+1}/G_i is abelian.

You might remember that a finite group G always has a composition series that's maximal in the sense that the G_{i+i}/G_i are all simple groups. In that case, the groups G_{i+1}/G_i are completely determined by G (Jordan-Hölder Theorem).

So if G is a finite group, then G is solvable if and only if its Jordan-Hölder factors are all abelian simple groups – thus each factor must be $\mathbf{Z}_p$ for a prime p.

Example 3.2. *Any abelian group is solvable.*

Example 3.3. *The dihedral groups D_{2n} are all solvable. The composition series is*

$$\{e\} \subset \mathbf{Z}_n \subset D_{2n}$$

The factor groups are $\mathbf{Z}_n$ and $\mathbf{Z}_2$. Both are abelian.

Example 3.4. *The symmetric groups S_2, S_3, S_4 are all solvable, but S_5 is not, nor is S_n for any $n \geqslant 5$. We have $S_2 \cong \mathbf{Z}_2$. We also have $S_3 \cong D_6$. We have in S_4:*

$$\{e\} \subset \mathbf{Z}_2 \subset \mathbf{Z}_2 \times \mathbf{Z}_2 \subset A_4 \subset S_4$$

The factor groups are $\mathbf{Z}_2, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_2$.

We have for S_5:

$$\{e\} \subset A_5 \subset S_5,$$

but this time A_5 is a simple group, of order 60. Thus A_5 is the smallest nonsolvable group.

Example 3.5. *After A_5, the next nonabelian simple group has order 168. It is the group of invertible 3×3 matrices with coefficients in $\mathbf{Z}_2$.*

Lemma 3.6. *Let G be a solvable group, and let H be a subgroup or a quotient of G. Then H is also solvable.*

4. The main theorem

Theorem 4.1. *Let F be a field of characteristic 0. Let E/F be a finite Galois extension, with group $G = \mathrm{Gal}(E/F)$. Then E/F is solvable if and only if G is a solvable group.*

Proof. We're only going to prove one direction: If E/F is solvable, then G is solvable.

Assume that E/F is solvable. Then E is contained in a field K, where

$$K = K_n \supset K_{n-1} \supset \cdots \supset K_0 = F,$$

where $K_{i+1} = K_i(\beta_i^{1/m_i})$, with $\beta_i \in K_i$. Let m be the LCM of all the m_i. Then let $F' = F(\zeta_m)$ be the splitting field of $x^m - 1$. Let

$$\begin{aligned} K'_0 &= F' \\ K'_1 &= K'_0(\beta_0^{1/m_0}) \\ K'_2 &= K'_1(\beta_1^{1/m_1}) \\ &\vdots \\ K'_n &= K'_{n-1}(\beta_{n-1}^{1/m_{n-1}}) \end{aligned}$$

Then K' contains K, and so it also contains E.

The extension K'/F is Galois: the conjugates of β_i^{1/m_i} are all of the form $\zeta\beta_i^{1/m_i}$, where ζ is an mth root of 1.

The extension K'_{i+1}/K'_i is abelian! We saw last time that $\mathrm{Gal}(K'_{i+1}/K'_i)$ is a subgroup of $\mathbf{Z}_{m_i}$. Finally, the extension F'/F is abelian, because it is a subgroup of $\mathbf{Z}_m^\times$.

We now have a tower of fields

$$K' = K'_n \supset K'_{n-1} \supset \cdots \supset K'_0 = F' \supset F,$$

where each field is abelian over the next. If $G' = \mathrm{Gal}(K'/F)$, then G' has a corresponding composition series:

$$\{e\} \subset H_{n-1} \subset \cdots \subset H_0 \subset G'$$

with each successive factor group abelian. Therefore the group G' is solvable.

Since E is a subfield of K', the group $G = \mathrm{Gal}(E/F)$ is a factor group of $G' = \mathrm{Gal}(K'/F)$. Since G' is solvable, so is G. □

The converse is very interesting, but a little bit harder.

The first consequence is that there is no "universal" quintic formula. There is a universal quadratic formula. If K is a field of characteristic 0, and $F = K(b, c)$, where b and c are indeterminates. Let E/F be the splitting field of the polynomial

$$x^2 + bx + c.$$

Then E/F is solvable. In fact it's radical: $E = F(\sqrt{b^2 - 4c})$.

We can do the same with $F = K(a, b, c)$, and let E/F be the splitting field of

$$x^3 + ax^2 + bx + c.$$

Then E/F is Galois, with group S_3. S_3 is a solvable group, so that E/F must be a solvable extension. This means that the roots of this polynomial are expressible in terms of the field operations and nested radicals.

The same is true for quartic polynomials. But not quintic polynomials, because S_5 is not solvable. If

$$F = K(s_1, \ldots, s_5),$$

and E is the splitting field of

$$x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5,$$

We learned that $E = K(r_1, \ldots, r_5)$, where the r_i are the roots of this polynomial, and that $\mathrm{Gal}(E/F) = S_5$, which permutes the r_i. The s_i are then the elementary symmetric polynomials in the r_i.

We have that E/F is not solvable. You cannot express the r_i in terms of radical expressions in the s_i.

So, there is no universal quintic formula. You might hold out hope that every particular quintic polynomial can be solved in radicals, though. However, this won't work either, as there are examples of polynomials with unsolvable Galois group:

Theorem 4.2. *Let E be the splitting field of the extension $2x^5 - 5x^4 + 5$ over $\mathbf{Q}$. Then $\mathrm{Gal}(E/\mathbf{Q}) \cong S_5$. Therefore $E/\mathbf{Q}$ is not a solvable extension.*

In fact, "most" irreducible quintic polynmials with rational coefficients have Galois group S_5, and are therefore not solvable by radicals.

Theorem 4.3. *Let $f(x) \in \mathbf{Q}[x]$ be a degree 5 irreducible polynomial with rational coefficients. Assume that $f(x)$ has three real roots and two complex ones. Then the Galois group of the splitting field of $f(x)$ is S_5.*

Proof. Let $F = \mathbf{Q}(\alpha)$ be the field obtained by adjoining just one root, and let E/F be the splitting field of $f(x)$, so that E contains all 5 roots.

Let $G = \mathrm{Gal}(E/\mathbf{Q})$, so that G is a subgroup of S_5. I might call the roots $\alpha = \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$, with α_1, α_2 being the complex roots. Let τ be complex conjugation, considered as an element of G. Then $\tau = (12)$ is a transposition. Since $[F : \mathbf{Q}] = 5$, we know that $[E : \mathbf{Q}] = \#G$ is divisible by 5. By the Sylow theorems we know that G must contain an element σ of order 5. We have that σ is a 5-cycle.

We want to know that a subgroup G of S_5 containing a transposition and a 5-cycle must be all of S_5. We can assume that $\sigma = (12345)$ (check this!). If we take $\tau = (12)$ and conjugate it by powers of σ, we find that $(23), (34), (45), (51)$ are also in G. It's easy to see that G has to contain the other transpositions as well, for instance:

$$(13) = (23)(12)(23).$$

Since S_5 is generated by its transpositions, we're done. □

The book suggests the example of $f(x) = 2x^5 - 5x^4 + 5$. This is irreducible by Eisenstein criterion (at $p = 5$), and it has three real roots (calculus).