Summaries, May 17 and 19

For this class, let's assume that our fields are subfields of the complex numbers. This assumption is easy to remove, but never mind.

Kummer Theory.

Theorem. Let p be a prime integer, and let F be a field that contains the pth root of unity $\zeta = \zeta_p = e^{2\pi i/p}$. Let K/F be a Galois extension of degree $[K : F] = p$. Then K can be obtained by adjoining a pth root: $K = F[\beta]$, with $\beta^p = b \in F$. (So $\beta = \sqrt[5]{b}$.

proof The Galois group G of K/F has order p, so it is a cyclic group. Let σ be a generator. We view K as an F-vector space of dimension $p = [K : F]$. Then the F-automorphism σ is a linear operator on K. Since $\sigma^p = 1$, the eigenvalues of σ are pth roots of unity, powers of ζ. Because an eigenvalue λ is in F, there is an eigenvector β in K with that eigenvalue. (The F-linear operator $\sigma - \lambda I$ is singular. Its determinant is zero. So there is an element in its kernel. Moreover, the eigenvalues aren't all equal to 1 because, in the field $\mathbb{C}$, σ is diagonalizable.

We choose an eigenvalue λ of σ, not equal to 1, and we let β be an eigenvector, so that $\sigma(\beta) = \lambda\beta$. Since $\lambda^p = 1$,

$$\sigma(\beta^p) = (\sigma(\beta))^p = (\lambda\beta)^p = \lambda^p\beta^p = \beta^p$$

This means that β^p is in the fixed field K^G, which is F. □

finding the pth root To obtain an element β whose pth power is in F, we start with an arbitrary element α of K. For $i = 0, ..., p-1$, let $\alpha_i = \sigma^i\alpha$. So $\sigma\alpha_i = \alpha_{i+1}$ for $i < p-1$, and $\sigma\alpha_{p-1} = \alpha_0$.

Let $\beta = \alpha_0 + \zeta\alpha_1 + \zeta^2\alpha_2 + \cdots + \zeta^{p-1}\alpha_{p-1}$.

$$\sigma\beta = \alpha_1 + \zeta\alpha_2 + \cdots + \zeta^{p-2}\alpha_{p-1} + \zeta^{p-1}\alpha_0 = \zeta^{-1}\beta$$

So unless β is the zero vector, it is is an eigenvector with eigenvalue ζ^{-1}. To obtain an eigenvector with value ζ, one replaces ζ by ζ^{-1}. If $\beta = 0$, one can try with a different α.

(In fact, K is the regular representation of G. It is direct one-dimensional irreducible representations, and $\frac{1}{p}\beta$ is the projection to the space with eigenvalue $-\zeta$. It won't be zero unless β is in the orthogonal space.)

Corollary. Let $f(x)$ be an irreducible cubic polynomial in $F[x]$ and let K be a splitting field.

(i) If the cube root of unity ζ_3 is in F and also the discriminant D of f is a square in F, then K is obtained by djoining a cube root to F. (The cube root of unity ζ_3 is $\frac{1}{2}(-1 + \sqrt{-3})$.)

(ii) In any case, K will be a subfield of a field $F[\sqrt{-3}, \sqrt{D}, \sqrt[3]{a}]$, where a is a combination of $1, \sqrt{-3}, \sqrt{D}, \sqrt{-3D}$.

Thus there will be a tower of fields

$$F \subset F_1 = F[\sqrt{-3}] \subset F_2 = F_1[\sqrt{D}] \subset F_3 = F_2[\sqrt[3]{a}]$$

such that the splitting field K is a subfield of F_3.

In particular, the roots of the cubic f can we written in terms of square roots and cube roots. Cardano gave a formula.

Cardano's formula For this formula, we assume that the coefficient of x^2 in the cubic polynomial f is zero. This can be achieved by a change of variables of the form $x = x + c$ for suitable c in F. We write

$$f(x) = x^3 + 3px + 2q$$

The coefficients 3 and 2 are there to avoid denominators. Then

$$\alpha = \sqrt[3]{q + \sqrt[2]{p^3 + q^2}} + \sqrt[3]{q - \sqrt[2]{p^3 + q^2}}$$

is a root of F.

For example, let $p = q = 1$. Cardano's formula for the root is

$$\alpha = \sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}}$$

However, Cardano's formula is both ambiguous as well as useless. Its ambiguity comes from the fact that there are two square roots of a given number and three cube roots. So there are 12 ways to read the formula, though f has only three roots. It is useless because it is much to hard to use it to compute.

The derivation of this formula requires some computation, but is otherwise easy. Let $\zeta = e^{2\pi i/3}$. Then $\zeta^{-1} = \zeta^2$. Let $\alpha_1, \alpha_2\alpha_3$ be the roots of f, The symmetric functions of α are $s_1(\alpha) = 0$, $s_2(\alpha) = 3p$, and $s_3(\alpha) = -2q$.

Now let

$$\beta = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 \quad \text{and} \quad \beta' = \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3$$

These are eigenvectors of σ with eigenvalues ζ^{-1} and ζ, respectively. So β^3 and β'^3 are fixed by $\sigma = (1\,2\,3)$. They are in $F' = F[\sqrt{-3}, \sqrt{D}]$. Also

$$\beta + \beta' = 2\alpha_1 + (\zeta + \zeta^2)(\alpha_2 + \alpha_3) =$$

$$= 2\alpha_1 - \alpha_2 - \alpha_3 = 3\alpha_1 - s_1(\alpha) = 3\alpha_1$$

So to represent α_1 as a sum of cube roots, we only need to compute β^3 and β'^3:

$$\beta^3 = (\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3)^3 = (\alpha_1^3+\alpha_2^3+\alpha_3^3)+3\zeta(\alpha_2^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1)+\zeta^2(\alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2)+6(\alpha_1\alpha_2\alpha_3)$$

Let $A = (\alpha_2^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1)$ and $B = (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)$. Since $\alpha_1^3 = -3p\alpha_1 - 2q$, $\beta^3 = -9ps_1(\alpha) - 6q + \zeta A + \zeta^2 B = -12q + \zeta A + \zeta^2 B$. We also have $\sqrt{D} = A - B$, and $s_2(\alpha) = 3p = A + B$. Putting these facts together, one determines β^3.

quartic equations

One can also solve an equation $f(x) = 0$ of degree 4 by roots. To do this, let $\alpha_1, ..., \alpha_4$ be the roots in a splitting field. We remember that the resolvent cubic $g(x)$ with roots $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, etc. has the same discriminant as the quartic polynomial f, and that if the roots of g are in an extension F' of F, then the Galois group of K/F' is a subgroup of D_2. It can be obtained by adjoining (at most) two square roots, call them $\sqrt{u}$ and $\sqrt{v}$. Thus K will be in the field F_6 obtained as follows:

$$F \subset F_1 = F[\sqrt{-3}] \subset F_2 = F_1[\sqrt{D}] \subset F_4 = F_3[\beta_1] \subset F_5 = F_4[\sqrt{u}] \subset F_6 = F_5[\sqrt{v}]$$

By Kummer Thory, F_4 can be obtained from F_3 by adjoining a cube root. So there is some useless formula for α_1 in terms of nested square roots and cube roots. I have no idea what it is.

the Main Theorem again

Let K be Galois extension of F, with Galois group G. The Main Theorem tells us that intermediate fields L, $F \subset L \subset K$ correspond to subgroups H of G, the correspondence being $L - -- > G(K/L) = H$ and $K^H < - - -H$.

There is one more fact to note: L is a Galois extension of F if and only if H is a normal subgroup of G. (It is always true that K is a Galois extension of L.) And, if so, then the Galois group $G(L/F)$ is the quotient group $\overline{G} = G/H$.

This isn't hard to prove. If L is a Galois extension of F, then it is a splitting field of some polynomial g that has roots $\gamma_1, ..., \gamma_k$ in L. An element σ of $G = G(K/F)$ permutes these roots, and since they generate L, σ restricts to an F-automorphism of L. That gives us the map $G \to \overline{G}$, with kernel H. etc...

Example. Let $F = \mathbb{Q}$, and let $K = F[\zeta_7]$, $\zeta_7 = e^{2\pi i/7}$. The Galois group $G = G(K/F)$ is a cyclic group of order 6. Let σ be the generator that sends $\zeta \to \zeta^3 \to \zeta^2 \to \zeta^6 \to \zeta^4 \to \zeta^5 \to \zeta$. It has a subgroup H of order 2, generated by σ^3, and H is normal beccause G is abelian. The quotient group G/H is cyclic of order 3. So the fixe field o L of H is a Galois extension of F with cyclic Galois group of order 3, and K is an Galois extension of L with cyclic Galis group of order 2.

Let ω be the cube root of unity. Then $L[\omega]$ is a Galois extenson of $F[\omega]$ of degree 3, so it can be obtained by adjoining a cube root. This means that ζ_7 is in a field obtained by a adjoining, in succession, a $\sqrt{\ }$, a $\sqrt[3]{\ }$, and another $\sqrt{\ }$.

Th analogous statement is true for the pth roots of unity, for an arbitrary prime p.

Proposition. Let p be a prime integer. There is a chain of fields $F \subset F_1 \subset \cdots \subset F_k$ such that F_i can be obtained from F_{i-1} by adjoinins a q_ith root, for some prime q_i, and such that ζ_p is in F_k.

The next lemma is also due to Galois:

Lemma. If a subgroup G of S_5 contains a 5-cycle σ and a transposition τ, then $G = S_5$.

The analogous statement is true for any prime $p \geq 5$, but never mind.

proof Say that τ is the transposition $(1\,2)$. Some power of the five cycle σ will carry 1 to 2. We replace σ by that power. Then since the numbering of the remaining indices is arbitrary, we may assume that $\sigma = (1\,2\,3\,4\,5)$. We compute:

$$\sigma\tau\sigma^{-1} = (1\,2\,3\,4\,5)(1\,2)(5\,4\,3\,2\,1) = (2\,3)$$

So $(2\,3)$ is in G. Conjugating by σ again shows that $(3\,4), (4\,5), (5\,1)$ are also in G. Similarly, $(2\,3)(1\,2)(2\,3) = (1\,3)$, etc. So $(2\,4), (3\,5), (4\,1), (5\,2)$ are in G. Every transposition is in G. The transpositions generate S_5, so $G = S_5$. □

Corollary. Let $F = \mathbb{Q}$. Let $f(x)$ be an irreducible polynomial of degree 5 in $F[x]$ with three real roots $\alpha_1, \alpha_2, \alpha_3$ and two complex roots α_4, α_5 Then the Galois group G of a splitting field K of f is the symmetric group S_5.

proof Since f is irreducible, $[K[\alpha_1] : F] = 5$, and therefore $[K : F]$ is divisible by 5. The order of G is equal to $[K : F]$, so it is also divisible by 5. It must contain an element of order 5, a 5-cycle. Next, let $L = F[\alpha_1, \alpha_2, \alpha_3]$. Adjoining α_4 to L is an extension of degree at most two. So $[K : L] \leq 2$. However, L is a subfield of the real numbers, while K is not. Therefore $L \neq K$. The degree $[K : L]$ is 2, and $G(K/L)$ is cyclic of order 2. Operating on the roots, its nonidentity element is the transposition $(4\,5)$. Since $G(K/L)$ is a subgroup of G, G contains a transposition and a 5-cycle. The lemma shows that $G = S_5$. □

Example. Let $F = \mathbb{Q}$. We exhibit a polynomial whose Galois group is S_5. We start with the polynomial $p(x) = (x^2 + 4)(x^2 - 4)x = x^5 - 16x$. It has three real roots $0, \pm 2$, but of course it is reducible. We note that the derivative $p'(x)$ has only two roots. So p has just one relative maximum and one relative minimum. Moreover, $p(1) = -15$. Therefore $f(x) = x^5 - 16x + 2$ also has three real roots, and it is irreducible. The Galois group of a splitting field K of f will be the symmetric group S_5. □

Theorem. Let K be the splitting field of an irreducible polynoial $f(x)$ of degree 5 over F. Assume that the Galois group $G = G(K/F)$ is either the symmetric group S_5 or the alternating group A_5. Also, suppose given a chain of field extensions $F \subset F_1 \subset \cdots \subset F_n$ such that, for every i, F_i is a Galois extension of F_{i-1} of prime degree q_i. Then there is no root of $f(x)$ in F_n.

This theorem shows that we can't write a root of f in terms of any number of nexted roots $\sqrt[q]{\ }$. There is no formula analogous to Cardano's formula for a root of f.

proof Let D be the discriminant of f. If $G = S_5$, we replace F by $F' = F[\sqrt{D}]$. The splitting field of f over F' will be the alternating group. So we may assume that G is the alternating group, a *simple group*. Let $\alpha_1, ..., \alpha_5$ be the roots of f in the splitting field K.

We consider a single Galois extension F' of F of prime degree p. We will show that the Galois group of the splitting field $K' = F'[\alpha_1, ..., \alpha_5]$ is again the alternating group. Then F' cannot contain a root of f. So no progress in solving the equation $f = 0$ is made by passing from F to F', and the theorem will follow by induction.

Say that $F' = F[\beta]$, where β is the root of an irreducible polynomial $g(x)$ of degree p in $F[x]$. Then $K' = F'[\alpha_1, ..., \alpha_5] = F[\alpha_1, ..., \alpha_5, \beta]$ So K' is the splitting field of the polynomial $f(x)g(x)$ over F. It is a Galois extension of F as well as a Galois extension of F'. We consider the diagram of field extensions

$$\begin{tikzcd}
K \arrow[r, "H'"] & K' \\
F \arrow[u, "G"] \arrow[r, "G'"] & F' \arrow[u, "H"']
\end{tikzcd}$$

All inclusions in this diagram are Galois extensions, and their Galois groups are indicated.

The field K' is a Galois extension of F. Let its Galois group be $\mathcal{G}$. Since K and F' are intermediate fields in the extension K'/F, the Galois groups H' and H are subgroups of $\mathcal{G}$. Since K and F' are Galois extension of F, H' and H are normal subgroups of $\mathcal{G}$, and $G = \mathcal{G}/H'$, and $G' = \mathcal{G}/H$. We are also given that $G = A_5$ and that G' is a cyclic group of order p.

Let σ be an element of $\mathcal{G}$, an F-automorphism of K'. We can restrict σ to K, to obtain an F-automorphism σ_1 of K. This element σ_1 is the automorphism obtained by letting σ operate on the roots $\alpha_1, ..., \alpha_5$. It is the residue of σ in $G = \mathcal{G}/H'$. Similarly, we can restrict σ to F', obtaining an element σ_2 of G'. Putting the maps $\mathcal{G} \to G$ and $\mathcal{G} \to G'$ together gives us a homomorphism $\mathcal{G} \to G \times G'$ that sends σ to the pair (σ_1, σ_2).

If $\sigma_1 = id$ and also $\sigma_2 = id$, then σ fixes the roots α_i and it also fixes β. Since K is generated by those elements, σ is the identity. The map $\mathcal{G} \to G \times G'$ is injective. So $|\mathcal{G}|$ divides $|G| \times |G'| = p|G|$. Also, since G is a quotient of $\mathcal{G}$, $|G|$ divides $|\mathcal{G}|$. Therefore $|\mathcal{G}|$ is either $|G|$ or $p|G|$ and $\mathcal{G}$ is either G or $G \times G'$. If $\mathcal{G} = G$, then the normal subgroup H of $\mathcal{G}$ is a normal subgroup of G and G has a quotient group isomorphic to the cyclic group G'. This is impossible because G is a simple group. Therefore the map $\mathcal{G} \to G \times G'$ is surjective as well as injective, and $\mathcal{G}$ is isomorphic to $G \times G'$. This being so, H is the kernel of the map $G \times G' \to G'$, and is isomorphic to the alternating group G, which is what we wanted to show. □