Summaries, May 3 and 5

Discriminant

As we know, the discriminant of the polynomial $f(x) = x^2 + bx + c$ is $D(f) = b^2 - 4c$, and it is zero if and only if f has a double root. What we weren't taught when I was in school is that, if α_1, α_2 are the roots of f, then the discriminant is also equal to $(\alpha_1 - \alpha_2)^2$.

The *discriminant* of a polynomial $f(x)$ of degree 3, with roots $\alpha_1, \alpha_2, \alpha_3$ is

$$D(f) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

and the discriminant of a polynomial of any degree is defined similarly, as the product of squares of the differences of the roots, $\prod_{i<j}(\alpha_i - \alpha_j)^2$.

The discriminant of the polynomial $f(x) = (x - u_1)\cdots(x - u_n)$ with variable roots $u_1, ..., u_n$, which is $\prod_{i<j}(u_i - u_j)^2$, is a symmetric polynomial in the roots, so it can be written as a polynomial in the elementary symmetric functions. Unfortunately, this polynomial is complicated. It is too complicated to remember, even for a cubic polynomial. Since the discriminant of a cubic is a homogeneous polynomial of degree 6, it is a combination of products of $s_!, s_2, s_3$ of total degree 6. It is

$$D(f) = 0s_1^6 + 0s_1^4 s_2 - 4s_1^3 s_3 + 1s_1^2 s_2^2 + 18s_1 s_2 s_3 - 4s_2^3 - 27s_3^2$$

The coefficients of the monomials that don't involve s_3 are easy to determine by the systematic method used in the proof of the Symmetric Functons Theorem. We set $u_3 = 0$:

$$D^\circ = (u_1 - u_2^2)u_1^2 u_2^2 = s_1^{\circ 2} - 4s_1^{\circ 2}\mathring{s}_2^{2} = \mathring{s}_1^{2}\mathring{s}_2^{2} - 4\mathring{s}_2^{3}$$

Therefore

$$D = s_1^2 s_2^2 - 4s_2^3 + s_3 q(s)$$

for some polynomial q of total degree 3. I don't know an easy way to determine the remaining three coefficients, but one way to do so is to compute the discriminant of some particular polynomials.

The discriminant of a cubic polynomial $f(x) = x^3 - a_1 x^2 + a_2 x - a_3$ is obtained by substituting $s_i = a_i$ into this formula. (But note the order of the indices and the alternating signs.)

For example, let $f(x)$ be the polynomial $x^3 + x^2 + x + 1$. The formula $x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1)$ shows that its roots are the fourth roots of unity $-1, i, -i$. So its discriminant is $(-1 + i)^2(-1 - i)^2(i + i)^2 = (1 - i^2)^2 4i^2 = -16$. In this case, $s_1, s_2, s_3 = -1, 1, -1$, and substitution into the formula for the discriminant in terms of the symmetric functions gives $1 - 4 + 18 - 4 - 27 = -16$ as well.

The roots of $x^3 + x^2 + x +!$ are distinct except in fields of characteristic 2. In characteristic 2, the discriminant becomes zero, and this reflects the fact that in characteristic 2, $x^3 + x^2 + x + 1 = (x + 1)^3$.

As I said, the formula for the discriminant of a cubic is too complicated to remember. It becomes simpler when the quadratic coefficient of F is zero. one can eliminate the quadratic coefficient of $x^3 - a_1 x^2 + a_2 x + a_3$ by the substitution $x = x + a_2/3$). Of course this changes the other coefficients. It is worth learning that the discriminant of the cubic $x^3 + px + q$ is

$$D = -4p^3 - 27q^2 \quad (= -4s_2^3 - 27s_3^2)$$

Automorphisms of a field extension

From now on we will assume that our fields have characteristic zero. They contain the rational numbers.

Let K be a field extension of a field F. An F-*automorphism* σ of K is an automorphism of K that restricts to the identity on F. So σ is a map $K \to K$ with these properties: $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$, and $\sigma(c) = c$ if c is in F. The set of F-automorphisms of K forms a group $G = G(K/F)$, the law of composition in the group being composition of functions. This group is called the *Galois group* of K over F.

I think that we have discussed the next lemma before:

Lemma 1. An irreducible polynomial $g(x)$ in $F[x]$ has no multiple root in any field extension.

proof A multiple root β of g is a root of g and of its derivative g'. Since g is irreducible, it generates the ideal of all polynomials with root β. The derivative g' cannot be in this ideal because it has lower degree than g. $\square$

Theorem 1. Let K be a splitting field over F of some polynomial $f(x$ in $F[x]$. Then the order of the Galois group is equal to the degree of the field extension: $|G(K/F)| = [K : F]$.

proof We use the Splitting Theorem and the Primitive Element Theorem. Let γ be a primitive element for the field extension. So $K = F[\gamma]$, and let $g(x)$ be the irreducible polynomial for γ over F, the irreducible monic polynomial in $F[x]$ that has γ as root. Then $K = F[\gamma] \approx F[x]/(g)$, the element γ corresponding to the residue $\overline{x}$ of x. If the degree of g is n, then $F[x]/(g)$ has dimension n as F-vector space. So $[K : F] = n = deg(g)$.

Since K is a splitting field and $g(x)$ has a root β in K, it splits completely in K. Let its roots in K be $\gamma_1, ..., \gamma_n$, with $\gamma = \gamma_1$. According to the lemma, the roots are distinct. So there are n of them. For any $i = 1, ..., n$, the field $F[\gamma_i]$ is also isomorphic to $F[x]/(g)$, so it has degree n over F. Since $F[\gamma_i] \subset K$ and both of these fields are extensions of $F$of dgree n, $K = F[\gamma_i]$ for every i.

We look at the two isomorphisms

$$K = F[\gamma_1] \xrightarrow{\approx} F[x]/(g) \xrightarrow{\approx} F[\gamma_i] = K$$

, the isomorphisms defined by $\gamma_1 \to \overline{x} \to \gamma_i$. They are the identity on F. The composed map $K \xrightarrow{\sigma_i} K$ is an F-automorphism of K. Now since all elements of $F[\gamma_1]$ can be written as polynomials in γ_1 with coefficients in F, an F-automorphism σ will be determined uniquely when we know the image $\sigma(\gamma_1)$, and that image must be a root of the same polynomial g. Therefore the automorphism σ_i, $i = 1, ..., n$, are the only ones, and $G(K/F)$ has order n. $\square$

Corollary 1. Let $g(x)$ be an irreducible polynomial in $F[x]$, and let γ be a root of g in a field extension K. Whether or not g splits completely in K, the order of the Galois group $G(K/F)$ is equal to the number of roots of g in that are in K.

The proof is the same. $\square$

Thus, if γ is the only root of g in K, then the only F-automorphism of K is the identity. For instance, when F is the field $\mathbb{Q}$ of rational numbers, g is the polynomial $x^3 - 2$, and γ is the real cube root of 2, the field $F[\gamma]$ has no automorphisms other than the identity.

Finite groups of automorphisms of a field

Let G be a finite group of automorphisms of a field K (of characteristic zero), and let $F = K^G$ be the fixed field. So an element σ of G has the properties tat were listed above: $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$, and $\sigma(c) = c$ if c is in F.

Theorem 2. Let G be a finite group of automorphisms of a field of charateristic zero, and let $F = K^G$ be the fixed field. Then the degree of the extension K/F is equal to the order of the group: $[K : F] = |G|$.

proof Let n be the order of G. The first step is to show that the degree $[K : F]$ is finite. Let α_1 be an element of K, and let $\alpha_1, ..., \alpha_r$ be its G-orbit. The order r of the orbit divides the order n of G, and the elements α_i are roots of the polynomial $f(x) = (x - \alpha_1) \cdots (x - \alpha_r)$, whose coefficients are symmetric functions in the orbit, so they are in F. Therefore $[F[\alpha_1] : F] \leq r$. (In fact, $[F[\alpha_1] : F]$ is equal to r.)

Now let $\alpha, \beta, ..., \delta$ be any finite set of elements of K. The field $L = F[\alpha, \beta, ..., \delta]$ they generate has finite degree over F. The degree is at most the product of the degrees of the extensions $F[\alpha]$, $F[\beta]$,...,$F[\delta]$ over F. This being so, the primitive element theorem tells us that $L = F[\gamma]$ for some γ. So $[L : F]$ divides n. Every finite set of elements of K generates a field extension of degree at most n. It follows that $[K : F] \leq n$.

So the degree $[K : F]$ is finite. We apply the primitive element theorem once more: $K = F[\gamma]$ for some element γ. Then, since every element of K can be written as a polynomial in γ with coefficients in F, an F-automorphism σ that fixes γ must be the identity. So the stabilizer of γ in G is $\{1\}$, and the orbit of γ has order $n = |G|$. If the orbit is $\gamma_1, ..., \gamma_n$ with $\gamma = \gamma_1$, then the polynomial $g(x) = (x - \gamma_1) \cdots (x - \gamma_n)$ has coefficients in F, as above. Moreover, g is an irreducible polynomial in $F[x]$. If $f(x) = p(x)q(x)$ with p, q in $F[x]$, then a root of f will be a root, either of p or of q, say a root of p. Then if $\sigma\gamma_1 = \gamma_i$, we will have $0 = \sigma p(\gamma_1) = p(\sigma\gamma_1) = p(\gamma_i)$. So γ_i is also a root for every i, which shows that $p = g$.

Thus $K = F[\gamma_1]$, and $[K : F] = \deg(g) = n = |G|$. □

Corollary 1. Let K be a splitting field of a polynomial over a field F, and let $G = G(K/F)$ be the Galois group of F-automorphisms of K. The fixed field K^G is equal to F.

proof Let n be the order of G. Theorem 1 tells us that $[K : F] = n$, and Theorem 2 tells us that $[K : K^G] = n$. Since the elements of G are F-automorphisms, $F \subset K^G$. Then

$$n = [K : F] = [K : K^G][K^G : F] = n[K^G : F]$$

So $[K^G : F] = 1$, and this implies that $F = K^G$. □

Automorphism of the field $\mathbb{C}(t)$ of rational functions

Let K be the field $\mathbb{C}(t)$ of rational functions – fractions of polynomials in t, and let X be the complex t-plane.

Let σ be an automorphism, and say that $\sigma(t) = p(t)/q(t)$, with p, q relatively prime polynomials. The rational function $\sigma(t)$ defines a map $X \to X$, or more precisely, a map from the set of points that aren't roots of $q(t)$ to X. This includes all but a finite set of points. The map σ sends a point $t = a$ to $p(a)/q(a) = b$. The fibre of σ over a point $t = b$ is the set of points a such that $p(a)/q(a) = b$, the set of points that are roots of the polynomial $g(t) = p(t) - bq(t) = 0$. If d is the maximum of the degrees of p and q, then g will have degree d for almost all values of b, and then the fibre will consist of d points.

There are special cases having to do with the possibilities that $g(t)$ has multiple roots or that $q(t)$ vanishes at a root of g. These accidents will occur only finitely often, but it is fussy to prove this. Let's not bother with the proof, and assume we know that for most values of b there will be d points in the fibre of σ.

Now, if σ is an automorphism of K, then σ^{-1} will also be an automorphism. It will also define a map $X \to X$ except on a finite set, and the composition $X \xrightarrow{\sigma} X \xrightarrow{\sigma^{-1}} X$ will be the identity map, wherever σ and σ^{-1} are defined. If σ has fibres of order greater than one, there is no way that the map σ^{-1} could exist. We conclude that the degree d of $p(t) - bq(t)$ must be 1, for almost all b. Therefore $p(t)$ and $q(t)$ must have degree at most 1. The automorphisms σ of $K = \mathbb{C}(t)$ send t to $\sigma(t) = \frac{at+b}{ct+d}$, for some invertible complex matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. These maps are called *fractional linear transformations*.

The law of composition of fractional linear transformations, which is composition of functions, is given by matrix multiplication. Here is the verification of this. Say that $\sigma(t) = \frac{at+b}{ct+d}$ and $\tau(t) = \frac{\alpha t+\beta}{\gamma t+\delta}$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \quad \text{and}$$

$$\sigma\tau(t) = \frac{a\frac{\alpha t+\beta}{\gamma t+\delta} + b}{c\frac{\alpha t+\beta}{\gamma t+\delta} + d} = \frac{a(\alpha t + \beta) + b(\gamma t + \delta)}{c(\alpha t + \beta) + d(\gamma t + \delta)} = \frac{(a\alpha + b\gamma)t + (a\beta + d\delta)}{(c\alpha + d\gamma)t + (c\beta + d\delta)}$$

The automorphism defined by a matrix A doesn't change when the matrix is multiplied by a nonzero scalar. The group of automorphisms of $K = \mathbb{C}(t)$ is the quotient group GL_2/H, where H is the subgroup of scalar matrices. It is called the *projective group*, and it is usually denoted by PGL_2.

We go back to finite group of automorphisms: The finite subgroup of PGL_2 are closely related to the finite rotation groups. There aren't very many, but they are interesting.

Example 1. Let G be the group generated by two elements σ, τ, where $\sigma(t) = \omega t$, ω being the cube root of unity $e^{2\pi i/3}$, and $\tau(t) = t^{-1}$. This group is isomorphic to the symmetric group S_3. We'll compute the fixed field $F = K^G$.

The orbit of t consists of the six rational functions $t, \omega t, \omega^2 t, t^{-1}, \omega t^{-1}, \omega^2 t^{-1}$. So t is a root of the polynomial f(x) = $(x - t)(x - \omega t)(x - \omega^2 t)(x - t^{-1})(x - \omega t^{-1})(x - \omega^2 t^{-1})$. The product of the first three factors is $x^3 - t^3$, and the product of the last three is $x^3 - t^{-3}$. So

$$f(x) = (x^3 - t^3)(x^3 - t^{-3}) = x^6 - (t^3 + t^{-3})x + 1 = x^6 - ut + 1$$

where $u = t^3 + t^{-3}$. The element u is a symmetric function in the orbit, so it is invariant. Then $\mathbb{C}(u) \subset F \subset K$. Since t is a root of f, it has degree 6 over $\mathbb{C}(u)$, and therefore $[K : \mathbb{C}(u)] = 6 = [K : F]$. This shows that

$[F : \mathbb{C}(u)] = 1$, so $F = \mathbb{C}(u)$. The fixed field is also a field of rational functions. This is an example of a famous theorem:

Lüroth's Theorem. Let K be the field $\mathbb{C}(t)$ of rational functions in one variables t, and let F be a subfield of K. If F is strictly larger than $\mathbb{C}$, thn it is a field of rational functions in one variable.

For example, one can take for F the field of rational functions in any two polynomials in t.

Unfortunately, we won't be able to prove this theorem here. It is usually proved in a course on algebraic curves.