Summaries, May 10 and 12

Recall that from now on our fields are assumed to have characteristic zero.

Let \( K \) be an extension of a field \( F \). The Galois group \( G(K/F) \) is the group of \( F \)-automorphisms of \( K \). A splitting field \( K \) of a polynomial \( f(x) \) with coefficients in \( F \) is also called a Galois extension of \( F \).

We have seen that if \( K \) is a Galois extension, then the order of the Galois group is equal to the degree of the extension: \( |G(K/F)| = [K:F] \).

It is also true that, for any finite field extension \( K/F \), \(|G(K/F)| \leq [K:F]\), and that if \( |G(K/F)| = [K:F] \), then \( K \) is a Galois extension of \( F \). However, we didn’t go over this in class.

We have also seen that, if \( G \) is a finite group of automorphisms of a field \( K \) and \( F = K^G \) is the fixed field, then \( [K : F] = |G| \). Therefore \( K \) is a Galois extension of \( F \).

**Corollary 1.** If \( K/F \) is a Galois extension and \( G \) is its Galois group, then \( F \) is the fixed field \( K^G \).

This is true because, by definition of an \( F \)-automorphism, \( F \subset K^G \). Then the formula \( [K:F] = [K:K^G][K^G:F] \) shows that \( [K^G:F] = 1 \), and therefore \( F = K^G \).

### adjoining square roots

Any field extension \( K/F \) of degree two is a splitting field, and it can be obtained by adjoining a square root. If \( \alpha \) is in \( K \) and not in \( F \), then \( F \subset F[\alpha] \subset K \), and by counting degrees, one sees that \( \alpha \) has degree 2 over \( F \) and that \( F[\alpha] = K \). If \( \alpha \) is a root of the quadratic polynomial \( f(x) = x^2 + bx + c \) and \( D \) is the discriminant \( b^2 - 4c \), then \( F[\alpha] = F[\sqrt{D}] \), where \( \delta = \sqrt{D} \).

Now let \( F \) be the field of rational numbers, and let \( K = F[\alpha, \beta] \), be the field obtained by adjoining two square roots to \( F \). We’ll use \( \alpha = \sqrt{3} \) and \( \beta = \sqrt{5} \) as an example. Then \( \beta \) isn’t in the field \( F[\alpha] \). It has degree 2 over that field, and \( [K : F] = 4 \).

We ask: Are there other square roots in \( K \)?

Of course, a number such as \( 7^2 \alpha \) shouldn’t be considered different. We should really ask for other field extensions of degree 2 that are contained in \( K \). The field \( F[\gamma] \), where \( \gamma = \alpha \beta = \sqrt{15} \) is an example of another such field.

The elements 1, \( \alpha, \beta, \gamma \) form a basis for \( K \) over \( F \). So to find all square roots algebraically, one would take a combination \( \delta = d + \alpha \alpha + \beta \beta + \gamma \gamma \) of this basis, and find \( a, b, c, d \) such that \( \delta^2 \) is in \( F \). This leads to the equations

\[
ad + 5bc = 0, \quad bd + 3ac = 0, \quad cd + ab = 0
\]

I’ve never tried to solve these equations, because there is a much easier method, which is to look at the Galois group.

The field \( K \) is the splitting field of the polynomial \( f(x) = (x^2 - 3)(x^2 - 5) \) over \( F \), so it is a Galois extension, and the Galois group \( G \) has order \( [K : F] = 4 \). Since \( \alpha^2 \) is in \( F \), an element \( \sigma \) of \( G \) must send \( \alpha \) to \( \pm \alpha \), and similarly, it must send \( \beta \) to \( \pm \beta \). And, when we know the images of \( \alpha \) and \( \beta \), \( \sigma \) is determined. Thus the four elements of \( G \) are 1, \( \sigma, \tau, \sigma \tau \), where

\[
\sigma(\alpha) = -\alpha, \quad \sigma(\beta) = \beta \\
\tau(\alpha) = \alpha, \quad \tau(\beta) = -\beta \\
\sigma \tau(\alpha) = -\alpha, \quad \sigma \tau(\beta) = -\beta
\]

Since \( \sigma^2 = \tau^2 = 1, G \) is the product \( C_2 \times C_2 \) of cyclic groups of order 2.

Now suppose that \( \delta = \sqrt{15} \) is in \( K \), with \( d \) an element of \( F \) that isn’t a square in \( F \), and let \( L = K[\delta] \). Then \( [L : F] = 2 \), and since \( F \subset L \subset K \), \([K : F] = 2 \). Also, \( K \) is a splitting field over \( L \). Let its Galois group (of order 2) be \( H \). Since \( F \subset L \), an \( L \)-automorphism of \( K \) is also an \( F \)-automorphism, so \( H \subset G \). Therefore \( L \) is the fixed field \( K^H \) of the subgroup \( H \) of \( G \) of order 2.

There are three subgroups of \( G(K/F) \) of order 2. They are generated by the three elements of order 2 in \( G \), which are \( \sigma, \tau, \) and \( \sigma \tau \). Therefore \( K \) contains three fields of degree 2 over \( F \), and they are \( F[\alpha], F[\beta] \) and \( F[\alpha \beta] \). There are no others.
cubic equations

Let $K$ be a splitting field over $F$ of an irreducible polynomial $f(x) = x^3 - a_1 qx^2 + a_2 x - a_3$ in $F[x]$ of degree 3, and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f$ in $K$, listed in an arbitrary order. We form a tower of fields:

$$F \subset F[\alpha_1] = F_1 \subset F[\alpha_1, \alpha_2] = F_2 \subset F[\alpha_1, \alpha_2, \alpha_3] = K$$

Since $f$ is an irreducible cubic polynomial in $F[x]$, the degree $[F_1 : F]$ is 3. Next, $f(x)$ has a root $\alpha_1$ in $F_1$. so in $F_1[x]$, $f(x) = (x - \alpha_1)q(x)$ for some quadratic polynomial $q(x)$ in $F_1[x]$ whose roots are $\alpha_2, \alpha_3$. That polynomial may be irreducible in $F_1[x]$ or not. If it is reducible, then $\alpha_2$ and $\alpha_3$ are in $F_1$, so $F_1 = F_2 = K$, and $[K : F] = 3$. On the other hand, if $q(x)$ is an irreducible element of $F_2[x]$, then $[F_2 : F_1] = 2$ and $[K : F] = 6$. In any case, the third root $\alpha_3$ will be in $F_2$, one reason being that the sum of the roots is the quadratic coefficient $a_1$ of $f$. It is in $F$, and $\alpha_3 = \alpha_1 - \alpha_1 - \alpha_2$. Summing up, the splitting field $K$ will have degree either 3 or 6 over $F$.

The Galois group $G = G(K/F)$ operates on the roots $\alpha_i$, and then because $K = F[\alpha_1, \alpha_2, \alpha_3]$, an element $\sigma$ of $G$ that fixes every one of the roots will be the identity automorphism. So $G$ operates faithfully on the roots, and by that operation, it becomes a subgroup of the symmetric group $S_3$. Since we know that $|G| = [K : F]$, we will have $G = S_3$ if $[K : F] = 6$, and $G = A_3$ if $[K : F] = 3$. The alternating group $A_3$ is the only subgroup of $S_3$ of order 3.

How can we tell which of these two possibilities we have in a particular case?

Recall that the discriminant of $f$ is the product $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ of the squares of the differences of the roots. The discriminant is an element of $F$. Its square root $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ is an element of $K$. If $\delta$ isn’t in $F$, then $K$ contains a quadratic extension $F[\delta]$ of $F$, and the degree $[K : F]$ is divisible by 2. Therefore $[K : F] = 6$ if $\delta$ isn’t in $F$.

Next, you will be able to check that a permutation $\sigma$ of the roots multiplies $\delta$ by the sign of that permutation. Therefore, if $\delta$ is an element of $F$, then an $F$-automorphism of $K$ must be an even permutation. In that case, $G = A_3$ and $[K : F] = 3$. So the element $\delta$ determines the degree $[K : F]$ and the Galois group $G(K/F)$.

intermediate fields

Let $K/F$ be a Galois extension. An intermediate field $L$ is a field extension of $F$ that is contained in $K$: $F \subset L \subset K$. As we see in the cases discussed above, the intermediate fields are useful tools for determining the structure of the extension. The Main Theorem describes these fields:

**Main Theorem.** Let $K/F$ be a Galois extension with Galois group $G$. There is a bijective correspondence between intermediate fields and subgroups of $G$. If $H$ is a subgroup of $G$, the corresponding intermediate field is the fixed field $K^H$, and if $L$ is an intermediate field, the corresponding subgroup is the Galois group $G(K/L)$. If a subgroup $H$ corresponds to the intermediate field $L$, then the degree $[K : L]$ is equal to the index $[G : H]$ of $H$ in $G$, and the degree $[L : F]$ is the order of $H$.

**proof** We must show two things:

- **If** $H$ is the Galois group $G(K/L)$ of an intermediate field $L$, then $L$ is its fixed field $K^H$.
- **If** $L$ is the fixed field $K^H$ of a subgroup $H$ of $G$, then $H$ is the Galois group $G(K/L)$.

Both are easy. If $K$ is a splitting field over $F$ of a polynomial $f(x)$ in $F[x]$, then it is also a splitting field for the same polynomial over an intermediate field $L$. Therefore $K/L$ is a Galois extension, and $|G(K/L)| = [K : L]$.

Let $L$ be an intermediate field, and let $H = G(K/L)$. Since $K$ is a Galois extension of $L$, $L$ is the fixed field of $H$.

Let $H$ be a subgroup and let $L$ be the fixed field $K^H$. Every element of $H$ fixes $L$, so it is an $L$-automorphism of $K$. Therefore $H \subset G(K/L)$. By the Fixed field Theorem, $[K : L] = |H|$. Therefore $|H| = |G(K/L)|$, which shows that $H = G(K/L)$. 

Let’s exhibit the correspondence in the case that $K$ is a splitting field of an irreducible cubic polynomial and $[K : F] = 6$. So the Galois group is the symmetric group $G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma \tau, \sigma^2 \tau\}$

with the usual relations $\sigma^3 = 1$, $\tau^2 = 1$, and $\tau \sigma = \sigma^2 \tau$. Let’s say that $\sigma = (1 \ 2 \ 3)$ and $\tau = (2 \ 3)$.

There are four proper subgroups, all cyclic: $< \sigma >$, $< \tau >$, $< \sigma \tau >$, and $< \sigma^2 \tau >$. Therefore there are exactly four intermediate fields in addition to $F$ and $K$. They are $F[\delta], F[\alpha_1], F[\alpha_2]$, and $F[\alpha_3]$. In
the correspondence between subgroups and intermediate fields, $< \sigma >$ corresponds to $F[\delta]$ and $< \tau >$ corresponds to $F[\alpha_1]$.

**Proposition 1.** Let $K$ be a splitting field of a polynomial $f(x)$ in $F[x]$, let $G$ be the Galois group $G(K/F)$, and let $\alpha_1, ..., \alpha_n$ be the roots of $f$ in $K$. Then $G$ operates on the set of roots.

(i) The operation of $G$ on the roots of $f$ is faithful: if an element $\sigma$ of $G$ fixes every root, then $\sigma$ is the identity. Therefore the operation on the roots embeds $G$ as a subgroup of the symmetric group $S_n$.

(ii) If $f(x)$ is an irreducible polynomial in $F[x]$, then the operation is transitive: for every $i = 1, ..., n$, there is an element $\sigma$ in $G$ such that $\sigma(\alpha_1) = \alpha_i$.

**proof (i)** If an $F$-automorphism $\sigma$ of $K$ fixes every root, then because $K$ is generated by the roots, $\sigma$ is the identity.

(ii) We must show that the roots form a $G$-orbit. Say that we have an orbit of order $k$. We number the roots so that the orbit is $\alpha_1, ..., \alpha_k$. The coefficients of the polynomial $g(x) = (x - \alpha_1) \cdots (x - \alpha_k)$ with these roots are symmetric functions in the orbit, so they are invariant, which means that $g$ has coefficients in $F$. If $f$ is irreducible, it generates the ideal of all polynomials with roots $\alpha_3$, so $f$ divides $g$, and therefore $f = g$. □

**quartic equations**

Let $K$ be a splitting field of an irreducible quartic polynomial $f(x) = x^4 - a_1 x^3 + a_2 x^2 - a_3 x + a_4$ in $F[x]$, and let $G$ be the Galois group of $K/F$. According to the proposition, $G$ embeds as a transitive subgroup of $S_4$. Therefore its order is divisible by 4, and of course $|G|$ divides $|S_4| = 24$. The order can be 4, 8, 12 or 24.

The transitive subgroups of $S_4$ are: $S_4$, $A_4$, $D_4$, $C_4$, $D_2$, and they have orders 24, 12, 8, 4, 4, respectively.

We form a tower of field extensions:

$$F \subset F[\alpha_1] \subset F[\alpha_1, \alpha_2] \subset F[\alpha_1, \alpha_2, \alpha_3] = K$$

The degrees of the field extensions are given above the $\subset$ symbols. The last root $\alpha_4$ is in the field $F[\alpha_1, \alpha_2, \alpha_3]$ because the sum of the roots is a coefficient of $f$, and is in $F$.

How can we decide, in a given case, which group is the Galois group? The first thing is to look at the discriminant $D$ of $f$. (Of course we don’t want to compute the discriminant unless it is absolutely necessary.) Let

$$\delta = \sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)$$

**Lemma 1.** With notation as above, $\delta \in F$ if and only if the Galois group $G$ is a subgroup of the alternating group $A_4$.

The proof is similar to the proof for cubic equations.

Next, one can use Lagrange’s resolvent cubic to determine whether or not $G$ contains an element of order 3. Let

$$\beta_1 = \alpha_1 \alpha_2 + \alpha_3 \alpha_4, \quad \beta_2 = \alpha_1 \alpha_3 + \alpha_2 \alpha_4, \quad \beta_3 = \alpha_1 \alpha_4 + \alpha_2 \alpha_3$$

These are all of the elements that are sums of products of the roots $\alpha_i$. Therefore they form an $S_4$-orbit. The coefficients of the polynomial

$$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3) = x^3 - b_1 x^2 + b_2 x - b_3$$

are symmetric functions in $\alpha_i$, so they are in the field $F$. For example, $b_2$, the sum of the roots $\beta_i$ is the symmetric function $s_2(\alpha)$, which is the coefficient $a_2$ of $x^2$ in $f$. It isn’t hard to determine the other coefficients in terms of the symmetric functions $s_i(\alpha) = \alpha_i$. You can do this as an exercise.

One happy accident is that the discriminant of $g$ is equal to the discriminant of $f$, from which it follows that the discriminant of $g$ isn’t zero. The discriminant of $f$ isn’t zero because $f$ is irreducible, but $g$ may be reducible. The discriminant of $g$ is $(\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2$. Using the following computation, it is easy to check that the two discriminants are the same:

$$(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) = \alpha_1 \alpha_2 + \alpha_3 \alpha_4 - \alpha_1 \alpha_3 - \alpha_2 \alpha_4 = \beta_1 - \beta_2$$
Proposition 2. (i) If the resolvent cubic $g$ is irreducible in $f[x]$, then $3$ divides $|G|$, and therefore $G = S_4$ or $A_4$.

(ii) If $g$ has one root in $F$, then $G$ is either $D_4$ or $C_4$.

(iii) If $g$ has three roots in $F$, then $G$ is $D_2$.

This isn’t hard to prove, but we ran out of time.