Math 5111 (Algebra 1)

Lecture #18 of 24 $\sim$ November 12th, 2020

Semidirect Products, Field Automorphisms

- Semidirect Products
- Field Automorphisms

This material represents §3.4.4 + §4.1.1-4.1.2 from the course notes.

Recall, I

Recall our results on semidirect products:

Theorem (Semidirect Products)

Let H and K be any groups, let $\sigma : K \to \mathrm{Aut}(H)$ be a group homomorphism with σ_k being the automorphism $\sigma(k)$ on H, and let G be the set of ordered pairs (h, k) for $h \in H$ and $k \in K$. Then G is a group with order $\#H \cdot \#K$ under the operation

$$(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1 \sigma_{k_1}(h_2),\ k_1 k_2).$$

Furthermore, the subset $\{(h, e) : h \in H\}$ is isomorphic to H and is a normal subgroup of G, while the subset $\{(e, k) : k \in K\}$ is isomorphic to K.
This group is called the semidirect product of H and K with respect to σ, and is denoted $H \rtimes_\sigma K$.

Recall, II

The point of the discussion last time was to identify when we can decompose a group G as a direct product or semidirect product.

- Specifically, suppose that we can decompose G as a product HK for two subgroups H and K where $H \cap K = \{e\}$.
- If both H and K are normal in G, then G is (isomorphic) to the direct product $H \times K$.
- If only H is normal in K, then instead G must be (isomorphic to) a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \mathrm{Aut}(H)$.

More Semidirect Products, I

Examples:

4. Let p be a prime. Let $H = \langle a \rangle \times \langle b \rangle$ be the direct product of two cyclic groups of order p and $K = \langle c \rangle$ be cyclic of order p.
   - Then H has the structure of an $\mathbb{F}_p$-vector space, and its group automorphisms are vector space isomorphisms.
   - This means that $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_p)$, with the action of a matrix being componentwise on the elements a and b.
   - Because $GL_2(\mathbb{F}_p)$ has order $(p^2-1)(p^2-p)$, it has a Sylow p-subgroup of order p.
   - We can realize this subgroup explicitly as the matrices of the form $\begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$ for $d \in \mathbb{F}_p$.

More Semidirect Products, II

Examples:

4. Let p be a prime. Let $H = \langle a \rangle \times \langle b \rangle$ be the direct product of two cyclic groups of order p and $K = \langle c \rangle$ be cyclic of order p.
   - Now let $\sigma : K \to \mathrm{Aut}(H)$ be the map with $\sigma(c) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which is well-defined since this matrix has order p in $GL_2(\mathbb{F}_p)$.
   - Explicitly, the associated automorphisms of H map $\sigma_c(a) = a$ and $\sigma_c(b) = ab$.
   - The resulting semidirect product $H \rtimes_\sigma K$ is a non-abelian group of order p^3, and it has a presentation $\langle a, b, c \ : \ a^p = b^p = c^p = e,\ ab = ba,\ cac^{-1} = a,\ cbc^{-1} = ab \rangle$.
   - One may show that it is isomorphic to the Heisenberg group from Homework 7.

More Semidirect Products, III

We can also use semidirect products to classify groups of a given order, if we can establish the existence of an appropriate normal subgroup and "complement" subgroup.

- In many cases, we will obtain several different possible choices for maps $\sigma : K \to \mathrm{Aut}(H)$.
- It can be shown that if K is cyclic and the images $\sigma_1(K)$ and $\sigma_2(K)$ inside $\mathrm{Aut}(H)$ are conjugate subgroups, then in fact the resulting semidirect products are isomorphic.
- Specifically, if $K = \langle a \rangle$ and $g\sigma_1(K)g^{-1} = \sigma_2(K)$, so that $g\sigma_1(a)g^{-1} = \sigma_2(a)^d$ for an integer d, then the map $\psi : H \rtimes_{\sigma_1} K \to H \rtimes_{\sigma_2} K$ given by $\psi(h, k) = ([\sigma_2]_g(h), a^d)$ is an isomorphism.

More Semidirect Products, IV

Example: Classify the groups of order 30.

- Since $30 = 2 \cdot 3 \cdot 5$, we must have $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 10\}$, and $n_5 \in \{1, 6\}$.
- However, we cannot have both $n_3 = 10$ and $n_5 = 6$, since then there would be 20 elements of order 3 and 24 elements of order 5, which is more than the number of elements in the group. Thus, $n_3 = 1$ or $n_5 = 1$.
- Therefore, the product of the Sylow 3-subgroup and Sylow 5-subgroup is also a subgroup of G (by our properties of subgroup products, since one of them is normal), and so G has a subgroup H of order 15.
- Since 3 does not divide $5 - 1$, from our classification of groups of order pq, H is cyclic.
- In fact, H is a normal subgroup of G, by problem 1a of Homework 8, since it has index 2.

More Semidirect Products, V

Example: Classify the groups of order 30.

- Now, there exists a Sylow 2-subgroup K of G.
- Then by order considerations, we see G must be isomorphic to a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \mathrm{Aut}(H)$.
- Since $H \cong \mathbb{Z}/15\mathbb{Z}$, one may verify that $\mathrm{Aut}(H) \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$, which is a product of a cyclic group of order 2 with a cyclic group of order 4.
- The map σ must send the nonidentity element $k \in K$ to an element of $\mathrm{Aut}(H)$ of order dividing 2.
- If σ is the trivial map, then G is abelian and isomorphic to $\mathbb{Z}/30\mathbb{Z}$.

More Semidirect Products, VI

Example: Classify the groups of order 30.

- We want $\sigma : K \to \mathrm{Aut}(H) \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$.
- If $\sigma(k) = (-1, 1)$, then the resulting automorphism maps $(a, b) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ to (a^{-1}, b). Then $\mathbb{Z}/5\mathbb{Z}$ is in the center of G, and G is isomorphic to $(\mathbb{Z}/5\mathbb{Z}) \times S_3$.
- If $\sigma(k) = (1, -1)$, then the resulting automorphism maps $(a, b) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ to (a, b^{-1}). Then $\mathbb{Z}/3\mathbb{Z}$ is in the center of G, and G is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times D_{2\cdot 5}$.
- If $\sigma(k) = (-1, -1)$, then the resulting automorphism maps $g \in (\mathbb{Z}/15\mathbb{Z})$ to g^{-1}. It is not hard to see that G is then isomorphic to $D_{2\cdot 15}$.
- Since these are all of the possible automorphisms, we see that up to isomorphism, there are four non-isomorphic groups of order 30: $\mathbb{Z}/30\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z}) \times S_3$, $(\mathbb{Z}/3\mathbb{Z}) \times D_{2\cdot 5}$, and $D_{2\cdot 15}$.

More Semidirect Products, VII

Example: Classify the groups of order 12.

- Since $12 = 2^2 \cdot 3$, we must have $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4\}$.
- First suppose that $n_3 = 4$. Then there are 8 elements of order 3, leaving only $12 - 8 = 4$ remaining elements, which must therefore form a unique Sylow 2-subgroup.
- Therefore, $n_2 = 1$, so the Sylow 2-subgroup H is normal in G.
- If K is any Sylow 3-subgroup, then $H \cap K = \{e\}$ since their orders are relatively prime, and since $\#H \cdot \#K = 12$, we have $HK = G$.
- Therefore, G is a semidirect product $H \rtimes_\sigma K$ for some nontrivial $\sigma : K \to \mathrm{Aut}(H)$.
- Otherwise, if $n_3 = 1$, then G is again a semidirect product, but now the Sylow 3-subgroup is normal and the Sylow 2-subgroup is not (necessarily).

More Semidirect Products, VIII

Example: Classify the groups of order 12.

1. $n_2 = 1$, $n_3 = 1$.

- Then G is nilpotent and the direct product of its Sylow subgroups. Since the Sylow subgroups have orders 4 and 3, they are both abelian.
- This means there are two isomorphism types for G: either G is isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$ or to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$.

More Semidirect Products, VIII

Example: Classify the groups of order 12.

2. $n_2 = 1$, $n_3 = 4$, $H = \langle a \rangle$ cyclic of order 4, $K = \langle c \rangle$ order 3.
   - Then $\mathrm{Aut}(H) \cong (\mathbb{Z}/4\mathbb{Z})^\times$ is cyclic of order 2.
   - But then if $K = \langle c \rangle$, there is no nontrivial map $\sigma : K \to \mathrm{Aut}(H)$, since $\sigma_c(a)$ would have order dividing both 2 and 3.
   - This is impossible, since then n_3 would be 1, not 4.

More Semidirect Products, IX

Example: Classify the groups of order 12.

3. $n_2 = 1$, $n_3 = 4$, $H = \langle a \rangle \times \langle b \rangle$ is Klein-4, $K = \langle c \rangle$ of order 3.
   - Then $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_2)$, of order $(2^2 - 1)(2^2 - 2) = 6$.
   - Thus, if $\sigma : K \to \mathrm{Aut}(H)$ is nontrivial, the image is a Sylow 3-subgroup of $GL_2(\mathbb{F}_3)$. Since these are all conjugate, the semidirect product is unique up to isomorphism.
   - Explicitly, if we take $\sigma : K \to \mathrm{Aut}(H)$ to be the map with $\sigma(c) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, then as an explicit automorphism we have $\sigma_c(a) = b$ and $\sigma_c(b) = ab$.
   - The resulting semidirect product $H \rtimes_\sigma K$ is a non-abelian group of order 12, and it has a presentation $\langle a, b, c \,:\, a^2 = b^2 = c^3 = e,\ ab = ba,\ cac^{-1} = b,\ cbc^{-1} = ab \rangle$.
   - In fact, this group is isomorphic to A_4 (take $a \mapsto (1\,2)(3\,4)$, $b \mapsto (1\,4)(2\,3)$, and $c \mapsto (1\,2\,3)$).

More Semidirect Products, X

Example: Classify the groups of order 12.

3. $n_2 = 3$, $n_3 = 1$, $K = \langle a \rangle$ cyclic of order 4, $H = \langle c \rangle$ of order 3.
   - Note here that $\mathrm{Aut}(H) \cong (\mathbb{Z}/3\mathbb{Z})^\times$ is cyclic of order 2, and generated by the inversion map $c \mapsto c^{-1}$.
   - Then there is one nontrivial homomorphism $\sigma : K \to \mathrm{Aut}(H)$, which has $\sigma_a(c) = c^{-1}$.
   - The resulting semidirect product is a non-abelian group of order 12, and it has a presentation $\langle a, c : a^4 = c^3 = e,\ aca^{-1} = c^{-1} \rangle$.

More Semidirect Products, XI

Example: Classify the groups of order 12.

4. $n_2 = 3$, $n_3 = 1$, $K = \langle a, b \rangle$ is Klein-4, $H = \langle c \rangle$ of order 3.

- There are three nontrivial homomorphisms $\sigma : K \to \mathrm{Aut}(H) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\}$: we can take $(a, b) \mapsto (1, -1), (-1, 1), (-1, -1)$.
- However, since their images are all the same (namely, $\{\pm 1\}$), the resulting semidirect products are isomorphic.
- If we take the first one, then the automorphisms act via $\sigma_b(a) = a$ and $\sigma_c(a) = a^{-1}$. So we get a presentation $\langle a, b, c : a^3 = b^2 = c^2 = e,\ bc = cb,\ bab^{-1} = a,\ cac^{-1} = a^{-1} \rangle$.
- In fact, this group is generated by c and $d = ab$, with presentation $\langle c, d : c^2 = d^6 = e,\ cdc^{-1} = d^{-1} \rangle$, which shows that it is isomorphic to the dihedral group $D_{2\cdot 6}$.

More Semidirect Products, XII

Example: Classify the groups of order 12.

- We have examined all of the possible cases.
- Since we can tell the cases apart by the number and structure of the Sylow subgroups, the groups are all non-isomorphic to one another.
- Thus, we conclude that there are five non-isomorphic groups of order 12: $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, $\mathbb{Z}/12\mathbb{Z}$, A_4, the nontrivial semidirect product $(\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$, and $D_{2\cdot 6}$.

From Groups to Fields

There is, of course, much more to be done in classifying finite groups of a given order.

- Our goal, however, is not to give exhaustive classifications for lots of group orders (although it is possible to do this in a number of cases using only Sylow's theorems and semidirect products, and some other observations about group actions and p-groups).
- Instead, the purpose is to have shown some of the tools that can be used to analyze the structure of finite groups of relatively small orders.
- Our reason for doing all of this group theory was so that we could study automorphism groups of fields.
- We have already witnessed the power of group actions for studying groups. Now we will use them to study fields.

Field Automorphisms, I

We begin by studying the collection of structure-preserving symmetries of a field K.

Definition

If K is a field, a (field) automorphism of K is a ring isomorphism of K with itself; explicitly, a field automorphism is a map $\sigma : K \to K$ that is a bijection and has $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$. The collection of all automorphisms of K is denoted $\mathrm{Aut}(K)$.

We will not worry about confusing the automorphism group of K as a group with the automorphism group of K as a field. We will essentially always intend the latter.

Field Automorphisms, II

Examples:

1. For $K = \mathbb{C}$, the complex conjugation map $\sigma(a + bi) = a - bi$, for $a, b \in \mathbb{R}$, is an automorphism of K. It is clearly a bijection, and it also respects addition and multiplication.
2. For $K = \mathbb{Q}(\sqrt{D})$ for squarefree D, the "conjugation map" $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$, for $a, b \in \mathbb{Q}$, is an automorphism of K. (If $D < 0$ then this map is simply complex conjugation.)
3. For $K = \mathbb{F}_{p^n}$ for a positive integer n, the pth-power Frobenius map $\sigma(x) = x^p$ for $x \in K$ is an automorphism of K. As we have previously mentioned, σ respects addition and multiplication and is injective, hence (since K is finite) it is a bijection.

Field Automorphisms, III

Based on our understanding of groups as collections of symmetries, we would expect $\mathrm{Aut}(K)$ to be a group under function composition[1]. Indeed, it is a group:

- The operation is well-defined, since the composition of two automorphisms is an automorphism.
- The operation is associative, since function composition is associative.
- There is an identity element, namely the identity map.
- Every element has an inverse, namely, the inverse function, which is also an automorphism.

[1] You may also expect it to be a group because I've already repeatedly referred to "the automorphism group of a field"!

Field Automorphisms, IV

Given a map from K to K, it is not hard to check whether it is an automorphism, but *a priori* it is not obvious how to construct automorphisms of K, nor how to compute the automorphism group $\mathrm{Aut}(K)$.

- As a first step, we observe that any automorphism of K must fix 0 and 1 (i.e., map 0 and 1 to themselves), and hence by a trivial induction must fix the prime subfield of K.
- In particular, this immediately tells us that $\mathrm{Aut}(\mathbb{Q})$ and $\mathrm{Aut}(\mathbb{F}_p)$ are both the trivial group.
- To extend this further, it will be useful to generalize our analysis to automorphisms that preserve field extensions.

Field Automorphisms, V

Definition

If K/F is a field extension, we define $\mathrm{Aut}(K/F)$ to be the set of automorphisms of K fixing F (i.e., the collection of $\sigma \in \mathrm{Aut}(K)$ such that $\sigma(a) = a$ for every $a \in F$).

- We can see that $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$: the identity map on K is clearly an element of $\mathrm{Aut}(K/F)$, and if $\sigma, \tau \in \mathrm{Aut}(K/F)$ then $\sigma\tau^{-1}$ is also in $\mathrm{Aut}(K/F)$ since $\sigma\tau^{-1}(a) = \sigma(\tau^{-1}(a)) = \sigma(a) = a$ for all $a \in F$.
- By our observations on the previous slide, since any automorphism of K fixes the prime subfield K', we have $\mathrm{Aut}(K) = \mathrm{Aut}(K/K')$.
- Thus, we may freely pass between speaking about automorphisms of K and automorphisms of K/K'.

Field Automorphisms, VI

A first observation toward computing all the automorphisms of an extension K/F is that any automorphism must be a linear transformation on K (though of as an F-vector space).

- Specifically, for $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(v+w) = \sigma(v) + \sigma(w)$ and $\sigma(\alpha v) = \alpha\sigma(v)$ for any $v, w \in K$ and $\alpha \in F$.
- Indeed, since σ is a bijection, in fact σ is an F-vector space isomorphism from K to itself.
- In particular, we may completely specify σ by its values on a basis for K/F.
- In fact, since σ also respects multiplication in K, it is enough to specify the value of σ on a set of generators for K/F as a field extension.

Field Automorphisms, VI

Although we can characterize an automorphism σ of K/F by its values on a set of generators for K/F, we cannot do so arbitrarily.

- For example, we cannot map any of the nonzero generators to 0, since σ must be a bijection.
- But even if we avoid trivial difficulties like that, other problems can arise.
- For example, suppose $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, and we want to try setting $\sigma(\sqrt{2}) = \sqrt{3}$ and $\sigma(\sqrt{3}) = \sqrt{2}$.
- If this were a field automorphism, we would also have to take $\sigma(1) = 1$ and $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = \sqrt{6}$.
- These choices do extend to a linear transformation, since we've now specified the values on a basis for $K/\mathbb{Q}$.
- However, the resulting map is not a field automorphism, because $\sigma(\sqrt{2} \cdot \sqrt{2}) = 2$ but $\sigma(\sqrt{2}) \cdot \sigma(\sqrt{2}) = 3$.

Field Automorphisms, VII

We would like determine exactly what choices will extend to an actual automorphism of the extension.

- We can glean some insight from the example of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- Specifically, because $\sigma \in \mathrm{Aut}(K/F)$ preserves addition and multiplication along with all elements of F, it will also preserve any algebraic relations between the generators that can be written using coefficients of F.
- Thus, for example, because $(\sqrt{2})^2 = 2$, the image $\sigma(\sqrt{2})$ must also satisfy the same algebraic relation: specifically, $\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2$.
- So in fact, the value $\sigma(\sqrt{2})$ can only be one of $\sqrt{2}$ and $-\sqrt{2}$.

In many cases, we can use this type of observation to compute all possible automorphisms.

Field Automorphisms, VIII

Example: Find all automorphisms of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

- By the discussion above, an automorphism σ of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is completely determined by the value $\sigma(\sqrt{2})$.
- Explicitly, we would have $\sigma(a+b\sqrt{2}) = \sigma(a)+\sigma(b)\sigma(\sqrt{2}) = a+b\cdot\sigma(\sqrt{2})$ for $a, b \in \mathbb{Q}$.
- Also as noted on the last slide, we must have $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$.
- But each of these choices does in fact extend to an automorphism of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$: the choice $\sigma(\sqrt{2}) = \sqrt{2}$ is satisfied by the identity automorphism, while the choice $\sigma(\sqrt{2}) = -\sqrt{2}$ is satisfied by the conjugation automorphism.

Field Automorphisms, IX

Example: Find all automorphisms of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

- We conclude that $|\mathrm{Aut}(K/\mathbb{Q})| = 2$, and so the automorphism group must be cyclic and isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
- Indeed, if τ represents the conjugation automorphism, then the structure of the group dictates that τ^2 will be the identity.
- Indeed, we have $\tau^2(a + b\sqrt{2}) = \tau(\tau(a + b\sqrt{2})) = \tau(a - b\sqrt{2}) = a + b\sqrt{2}$, as claimed.

Remark: If D is a squarefree integer, the same arguments with D in place of 2 show that for $K = \mathbb{Q}(\sqrt{D})$, the automorphism group $\mathrm{Aut}(K/\mathbb{Q})$ also has order 2 and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Field Automorphisms, X

Example: Find all automorphisms of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

- As above, an automorphism σ of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is completely determined by the value $\sigma(\sqrt[3]{2})$.
- Since $(\sqrt[3]{2})^3 - 2 = 0$, applying σ to both sides yields $\sigma(\sqrt[3]{2})^3 - 2 = 0$, so $\sigma(\sqrt[3]{2})$ is a root of $p(x) = x^3 - 2$.
- However, the other two roots of this polynomial (inside $\mathbb{C}$) are $\sqrt[3]{2} \cdot \zeta_3$ and $\sqrt[3]{2} \cdot \zeta_3^2$ for ζ_3 a primitive 3rd root of unity. These elements are not in $\mathbb{Q}(\sqrt[3]{2})$, since they are not real.
- Therefore, the only possibility is to have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, and then σ is simply the identity map.
- Thus, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group.

Remark: If K is either of $\mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3)$ or $\mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3^2)$, then $\mathrm{Aut}(K/\mathbb{Q})$ is also the trivial group. This follows by the same argument, since the polynomial $x^3 - 2$ only has one root in K.

Field Automorphisms, XI

Rather than doing more *ad hoc* examples, let's formalize the ideas. We will first establish a lemma that will be useful for constructing isomorphisms:

Lemma (Lifting Isomorphisms)

Let $\varphi : E \to F$ be an isomorphism of fields. If α is algebraic over E with minimal polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n \in E[x]$, and β is algebraic over F with minimal polynomial $q(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F[x]$, then there is a unique isomorphism $\tilde{\varphi} : E(\alpha) \to F(\beta)$ extending φ (i.e., such that $\tilde{\varphi}|_E = \varphi$) and such that $\varphi(\alpha) = \beta$.

We essentially proved this in the course of establishing the uniqueness of splitting fields. But it's been a while, so I'll go through the argument.

Field Automorphisms, XII

Proof:

- Since the minimal polynomial has degree n, that means $[E(\alpha) : E] = n$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$, and similarly $[F(\beta) : F] = n$ with basis $\{1, \beta, \beta^2, \ldots, \beta^n\}$.
- Then any isomorphism $\tilde{\varphi}$ extending φ with $\tilde{\varphi}(\alpha)$ must have $\tilde{\varphi}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = \varphi(c_0) + \varphi(c_1)\beta + \cdots + \varphi(c_{n-1})\beta^{n-1}$ for $c_i \in E$, so there is at most one possible map $\tilde{\varphi}$.
- On the other hand, one may verify that this map $\tilde{\varphi}$ (which is well defined) does indeed respect addition and multiplication, and has an inverse map $\tilde{\varphi}^{-1}(d_0 + d_1\beta + \cdots + d_{n-1}\beta^{n-1}) = \varphi^{-1}(d_0) + \varphi^{-1}(d_1)\alpha + \cdots + \varphi^{-1}(d_{n-1})\alpha^{n-1}$, so $\tilde{\varphi}$ is in fact an isomorphism.

Field Automorphisms, XIII

In the situation where we take the map φ to be the identity, we obtain a characterization of the automorphisms of a simple algebraic extension:

Theorem (Automorphisms of Simple Algebraic Extensions)

Suppose α is algebraic over F with minimal polynomial $m(x)$, and $K = F(\alpha)$: then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is also a root of $m(x)$ in K.
Conversely, if β is any other root of $m(x)$ in K, then there exists a unique automorphism $\tau \in \mathrm{Aut}(K/F)$ with $\tau(\alpha) = \beta$.
Therefore, $|\mathrm{Aut}(K/F)|$ is equal to the number of roots of $m(x)$ in K, and is (in particular) finite and at most $[K : F]$.

This business about counting the number of roots should remind you of separability, which will come into play in a little while.

Field Automorphisms, XIV

Proof:

- Suppose that $m(x) = a_n x^n + \cdots + a_1 x + a_0$ with the $a_i \in F$. Note that $\sigma(a_i) = a_i$ since σ fixes F.
- Then $m(\sigma(\alpha)) = a_n \sigma(\alpha)^n + \cdots + a_1 \sigma(\alpha) + a_0 = \sigma(a_n \alpha^n) + \cdots + \sigma(a_1 \alpha) + \sigma(a_0) = \sigma(a_n \alpha^n + \cdots + a_1 \alpha + a_0) = \sigma(0) = 0$ and so $\sigma(\alpha)$ is also a root of $m(x)$.
- For the second statement, suppose β is another root of $m(x)$ in K. If we apply the isomorphism lifting lemma with $E = F$ (so that the isomorphism φ is the identity map), then we see that there is a unique isomorphism $\tau : F(\alpha) \to F(\beta)$ such that $\tau(\alpha) = \beta$. Since $F(\alpha) = K = F(\beta)$, the map τ is an automorphism of K.
- We then have a bijection between roots of $m(x)$ in K and $\mathrm{Aut}(K/F)$, and since $m(x)$ has degree $[K : F]$, we conclude that $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Field Automorphisms, XV

Using this characterization, we can compute all the automorphisms of a simple algebraic extension, and then (at least in principle) we may determine the structure of the automorphism group.

- The hard part is determining how many roots of the minimal polynomial of the generator α are actually in the field $K = F(\alpha)$.
- Once we have identified them all, however, we need only count how many of them there are. Then by the isomorphism lifting lemma, we get an automorphism of K/F for each root.
- To find the group structure, we can then write down the action of each automorphism on α and see what happens when we compose them. This is where knowledge of the possible groups of a given order will be very useful.

Field Automorphisms, XVI

Example: Identify the elements of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q})$.

- As we have previously computed, $\sqrt{2}+\sqrt{3}$ is a root of the polynomial $m(x) = x^4 - 10x^2 + 1$.
- Also, since $K = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ has degree 4 over $\mathbb{Q}$, we see $m(x)$ is irreducible over $\mathbb{Q}$.
- By applying the quadratic formula twice, we can see that the four roots of $m(x)$ are $\pm\sqrt{2} \pm \sqrt{3}$, all of which are in K.
- Hence there are 4 automorphisms of $K/\mathbb{Q}$, obtained by mapping $\sqrt{2}+\sqrt{3}$ to any one of the other four roots of $m(x)$.

Field Automorphisms, XVI

Example: Identify the group structure of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q})$.

- One option is to compute the actions of the four automorphisms just from their behavior on $\sqrt{2}+\sqrt{3}$.
- Clearly, the map sending $\sqrt{2}+\sqrt{3}$ to itself will extend to the identity automorphism.
- But it is not so clear how to compute the compositions of the other automorphisms, since we only know their values on $\sqrt{2}+\sqrt{3}$.
- So in fact, we will really need to calculate their values on a basis of the extension: then it will be quite easy to see how they compose.

Field Automorphisms, XVII

Example: Identify the group structure of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q})$.

- For the map σ with $\sigma(\sqrt{2}+\sqrt{3}) = -\sqrt{2}+\sqrt{3}$, we see $\sigma(5+2\sqrt{6}) = \sigma((\sqrt{2}+\sqrt{3})^2) = \sigma(\sqrt{2}+\sqrt{3})^2 = (\sqrt{2}-\sqrt{3})^2 = 5-2\sqrt{6}$, and $\sigma(11\sqrt{2}+9\sqrt{3}) = \sigma((\sqrt{2}+\sqrt{3})^3) = \sigma(\sqrt{2}+\sqrt{3})^3 = (\sqrt{2}-\sqrt{3})^3 = 11\sqrt{2}-9\sqrt{3}$.
- So since σ fixes $\mathbb{Q}$, by taking appropriate linear combinations we can conclude that $\sigma(\sqrt{2}) = \sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$, and $\sigma(\sqrt{6}) = -\sqrt{6}$.
- Thus σ is the map with $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$.

Field Automorphisms, XVIII

Example: Identify the group structure of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q})$.

- In a similar way, we can see that the map τ with $\tau(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$ has $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$, and thus τ is the map with $\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$.
- Since σ has $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$, we can see that $\sigma\tau$ is the map with $\sigma\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$.
- Notice then that σ^2, τ^2, and $(\sigma\tau)^2$ are each the identity map, and also that $\tau\sigma = \sigma\tau$.
- So we can see $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{e,\sigma,\tau,\sigma\tau\}$ is isomorphic to the Klein 4-group.

Field Automorphisms, XIX

The procedure in this last example only applies to simple extensions, and in any case it seems likely that it might be easier to analyze the automorphisms of $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ using the simpler generators $\sqrt{2}$ and $\sqrt{3}$.

- We know that any automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ must map $\sqrt{2}$ to $\pm\sqrt{2}$ and must also map $\sqrt{3}$ to $\pm\sqrt{3}$, and since $\sqrt{2}$ and $\sqrt{3}$ generate the field, these choices completely determine the automorphism.
- But since these two choices yield at most 4 possible automorphisms, and there actually are 4 automorphisms from our calculations above, all 4 possible choices must in fact extend to automorphisms.

Field Automorphisms, XX

Thus in fact, we can equivalently describe the four automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ as the four possible maps sending $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$.

- We can see that the automorphism mapping $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$ is the identity map.
- If we let σ be the automorphism mapping $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$, then $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = -\sqrt{6}$, and so explicitly σ is the map we found before, with $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$.
- Likewise, if we let τ be the automorphism mapping $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$, then $\tau(\sqrt{6}) = \tau(\sqrt{2})\tau(\sqrt{3}) = -\sqrt{6}$, so $\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$.
- We can then immediately determine the group structure by composing σ and τ as we did above.

Field Automorphisms, XXI

Notice that our computation of the automorphisms in the second version of the example relied on the knowledge that there were actually 4 automorphisms of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

- We could, alternatively, have constructed these automorphisms explicitly via the isomorphism lifting lemma on simple extensions.
- To construct σ, first observe that $x^2 - 2$ is the minimal polynomial of both $\sqrt{2}$ and $-\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$, since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$.
- Then by the isomorphism lifting lemma applied to the identity map on $\mathbb{Q}(\sqrt{3})$, there is an automorphism σ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\mathbb{Q}(-\sqrt{2}, \sqrt{3})$ that fixes $\mathbb{Q}(\sqrt{3})$ and maps $\sqrt{2}$ to $-\sqrt{2}$. This automorphism then has $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$, so it extends to the automorphism we identified above.

Field Automorphisms, XXII

We can also construct the other automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ in this way.

- Explicitly, we can construct τ by observing that $x^2 - 3$ is the minimal polynomial of both $\sqrt{3}$ and $-\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$.
- Thus, there is an automorphism τ of $\mathbb{Q}(-\sqrt{2}, \sqrt{3})$ that fixes $\mathbb{Q}(\sqrt{2})$ and maps $\sqrt{3}$ to $-\sqrt{3}$.
- We can also construct $\sigma\tau$ by lifting the conjugation automorphism on $\mathbb{Q}(\sqrt{3})$: explicitly, $x^2 - 2$ is the minimal polynomial of both $\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$ and of $-\sqrt{2}$ over $\mathbb{Q}(-\sqrt{3})$.
- Then there is an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that extends the conjugation automorphism on $\mathbb{Q}(\sqrt{3})$ (sending $\sqrt{3}$ to $-\sqrt{3}$) to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that maps $\sqrt{2}$ to $-\sqrt{2}$.

Field Automorphisms, XXIII

We can use a similar procedure to the one we gave for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ to construct automorphisms of other composite extensions by lifting isomorphisms of appropriate subfields.

- The idea is quite similar: we start with an isomorphism on the bottom, and then add generators one at a time.

Field Automorphisms, XXIV

Example: Construct a nontrivial automorphism of $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ over $\mathbb{Q}$.

- There are various choices to be made here.
- Let's start with the isomorphism of $E = \mathbb{Q}(\sqrt[3]{2})$ with $E' = \mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3)$ that maps $\sqrt[3]{2}$ to $\sqrt[3]{2} \cdot \zeta_3$.
- Since the minimal polynomial of ζ_3 over both E and E' has degree 2 (since ζ_3 is a root of the quadratic polynomial $x^2 - x + 1$ and ζ_3 is not in E or E'), we can then lift this isomorphism to obtain an automorphism σ of K with $\sigma(\zeta_3) = \zeta_3$ and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \zeta_3$.

Field Automorphisms, XXV

Example: Construct a nontrivial automorphism of $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ over $\mathbb{Q}$.

- We have an automorphism σ of K with $\sigma(\zeta_3) = \zeta_3$ and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \zeta_3$.
- We can write out the full action of σ on K using the $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \sqrt[3]{2}\zeta_3, \sqrt[3]{4}\zeta_3\}$: since $\sigma(1) = 1$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$, $\sigma(\sqrt[3]{4}) = \sqrt[3]{4}\zeta_3^2$, $\sigma(\zeta_3) = \zeta_3$, $\sigma(\sqrt[3]{2}\zeta_3) = \sqrt[3]{2}\zeta_3^2$, and $\sigma(\sqrt[3]{4}\zeta_3) = \sqrt[3]{4}\zeta_3^3 = \sqrt[3]{4}$.
- Then $\sigma(c_1 + c_2\sqrt[3]{2} + c_3\sqrt[3]{4} + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3 + c_6\sqrt[3]{4}\zeta_3) = c_1 + c_2\sqrt[3]{2}\zeta_3 + c_3\sqrt[3]{4}\zeta_3^2 + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3^2 + c_6\sqrt[3]{4}$ for arbitrary constants $c_i \in \mathbb{Q}$.
- Observe (in particular) how unpleasant it would be to verify that σ is actually an automorphism of K using only this latter description!

Field Automorphisms, XXVI

It is not immediately obvious, however, that every automorphism of an arbitrary finite-degree extension actually arises in this fashion.

- Suppose that K/F is a finite-degree extension: as we have shown, $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$ that are algebraic over F.
- Since each automorphism σ of K/F is determined by its values on $\alpha_1, \ldots, \alpha_n$, and $\sigma(\alpha_i)$ must be a root of the minimal polynomial of α_i, we see that there are only finitely many automorphisms of K/F, and so $\mathrm{Aut}(K/F)$ is a finite group.
- If $\beta_1, \beta_2, \ldots, \beta_n$ are other roots of the minimal polynomials of the α_i in K, we might attempt to use the isomorphism lifting lemma to construct an automorphism of K that maps α_i to β_i for each i.
- But, sadly, this is not always possible!

Field Automorphisms, XXVII

To illustrate the issues, consider the field $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt{2})$.

- If we take $\alpha_1 = \sqrt[4]{2}$ and $\beta_1 = -\sqrt[4]{2}$, with $\alpha_2 = \sqrt{2}$ and $\beta_2 = -\sqrt{2}$, then each β_i is a root of the corresponding minimal polynomial of α_i over $\mathbb{Q}$.
- However, there is no automorphism τ of K that maps α_1 to β_1 and α_2 to β_2, because we would have $\tau(\sqrt{2}) = \tau(\alpha_2) = \beta_2 = -\sqrt{2}$, but also $\tau(\sqrt{2}) = \tau(\alpha_1^2) = \beta_1^2 = \sqrt{2}$.
- The issue here is that there is an algebraic relation between the generators of this field (namely, $\sqrt{2} = (\sqrt[4]{2})^2$) that must also be respected by the automorphism, so we cannot make our choices arbitrarily.
- Of course, this is a mildly fictitious issue, because we could have just used a single generator $\sqrt[4]{2}$. (But you get the idea.)

Field Automorphisms, XXVIII

There is also another related difficulty in this example of $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt{2})$, namely, that some isomorphisms of subfields cannot be lifted to the full field.

- For example, the conjugation map $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ sending $\sqrt{2}$ to $-\sqrt{2}$ cannot be lifted to an automorphism of K, because there is no possible value of $\tilde{\sigma}(\sqrt[4]{2})$: its square would necessarily be $-\sqrt{2}$, but there is no such element in K.
- On the other hand, there is such an element (namely, $\sqrt[4]{2} \cdot i$) in the splitting field $\mathbb{Q}(\sqrt[4]{2}, i)$.
- This suggests that working with splitting fields may solve this particular problem.
- In fact, we have already shown that for splitting fields, we can always lift isomorphisms on appropriate subfields to the full splitting field. So, we will pick up with automorphisms of splitting fields next time.

Summary

We discussed some more examples of semidirect products and classified the groups of some small orders.

We introduced the automorphism group of a field extension and described methods for computing it in some cases.

Next lecture: Automorphisms of splitting fields, Galois groups, fixed fields.