Abstract Algebra
: special homework: 13

2024.12.17

In our course we mainly focus on field with Char= 0.

This is a special homework for all of you, mainly based on the book of *Abstract Algebra* by David S. Dummit and Richard M. Foote section 14.1. You do not need to submit this homework although I will write a solution for it. I find some of you are not familiar with the concepts of field theory and I hope this homework will help you to understand it better.

Before we start, I want to ask you a question: what did Galois tell us?

To know this story we have to know some background: at that time, many mathmeticians were keen on solving polynomial equations. Consider what can we do to solve a polynomial equation:

$$x - 3 = 0$$

I guess now you think: "Come on! Don't traet me like a fool! It's so easy! The answer is obviously 3!" Yes, everybody knows that. And the process is, you add 3 from both sides of the equation and then you get the solution $x = 3$. In this process the operations we used are only addition (and maybe subtraction if I use $x + 3 = 0$ as an exercise). OK, what about I set it harder, like:

$$2x - 3 = 0$$

I think I might have made you feel angry. "Are you kidding me?" Please calm down. What I want to say is, to solve this equation we use 4 operations now: addition, subtraction, multiplication and division. But wait, what if I set it even harder?

$$x^2 - 3 = 0$$

Ok, now you are really angry. "What the hell is this?" I know you are angry, but please calm down again. Now we have to use 5 operations: addition, subtraction, multiplication, division and

exponentiation. i.e. We use all operations of this tuple: $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$ (In this case $n = 2$). A long time ago, mathematicians had already proven that for a quadratic equation $ax^2 + bx + c = 0$, there is a formula to find the solution:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Only use operations in this tuple: $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$ (In this case $n = 2$). Many years after that, they also found the formula for a cubic equation $ax^3 + bx^2 + cx + d = 0$ and a quartic equation $ax^4 + bx^3 + cx^2 + dx + e = 0$. But in a long period of time they didn't find the formula for a general quintic equation $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ which only use $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$ (in finitely many steps, if it can be this is called soluble by radicals). But many of those mathematicians truely believe that any polynomial equation of any degree is soluble by radical.

The first confusion appears as: since $\mathbb{C}$ is a algebraically field why a general polynomial with degree more that 4 "has no root" ? Now I think you know that this is just a misstatement. It's not "has no root" , it's "there exist roots can not be express by radicals" or "you can not use operations $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$ on all the coefficients in finitely many steps to express all its roots" . In other words, find the general formula based on $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$.

Since everyone failed in finding this formula, some mathematicians started to doubt whether this is true. And Abel, Ruffini and Galois started to study the solvability of polynomial equations. All of them are great mathematicians and Galois is the most famous one since he is the first one to translate this problem of solvability of a equation to the solvability of a group. In fact, he researched this problem by consider the extension of fields and established the correspondence between field extension and related group which is called Galois group.

Among these operations: $\{+, -, \times, \div, \sqrt[n]{\cdot}\}$, one is special:

$$\sqrt[n]{\cdot}$$

Since a filed is closed under $\{+, -, \times, \div\}$ but not under $\sqrt[n]{\cdot}$. So this operation $\sqrt[n]{\cdot}$ means you (may) created" a new element over the field. Or, you make an extension of given field. Galois find that this operation is related to "cyclic extention" , which is also related to its Galois group which is also cyclic. In other words, an element can be express by radicals $\Rightarrow$ you use $\sqrt[n]{\cdot}$ with (maybe different n's) finitely many times $\Rightarrow$ get the "biggest" filed from the given filed by finitely many times cyclic field extentions $\Rightarrow$ the "biggest" Galois group is a group extension by cyclic groups in finitely many steps $\Rightarrow$ this "biggest" Galois group is soluble.

I think now you can have a naive but intuitively feeling of Galois theory. I will give you formal definitions and theorems of what we discussed above:

Definition 1. *The extension K/F is said to be cyclic if it is Galois with a cyclic Galois group.*

Definition 2. *If K/F is a cyclic extension of degree n of a field F which contains a primitive nth root of unity ζ, then there exists an $x \in E$ with $x^n \in K$ and $E = K(x)$. i.e. Cyclic extensions are radical extensions.*

Definition 3. *An element α which is algebraic over F can be expressed by radicals or solved for in terms of radicals if α is an element of a field K which can be obtained by a succession of simple radical extensions*

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K$$

where $K_{i+1} = K_i\left(\sqrt[n]{a_i}\right)$ for some $a_i \in K_i, i = 0, 1, \ldots, s-1$. Here $\sqrt[n]{a_i}$ denotes some root of the polynomial $x^{n_i} - a_i$. Such a field K will be called a root extension of F.

Definition 4. *A polynomial $f(x) \in F[x]$ can be solved by radicals if all its roots can be solved for in terms of radicals.*

Theorem 5. *The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.*

All definitions and theorems above is the "goal" of learning Galois theory. You will eventually learn those things in this course or in some other course like "abstract algebra II". If you find this formal things is hard to understand or prove please take it easy: we will not examine what we do not learn at the final exam. So why I talked a lot about these and listed them here? Because I want everyone konw "why we need to learn this". Actually this is like, emmm, if you want to have a trip then the first thing you need to do is to know where you want to go. In mathematics we call this as your "motivation".

As for your "homework", I would like to help everyone review some of the content related to Galois theory that you have already learned. Since this part contains many new concepts, we need to go over them repeatedly in order to fully grasp and understand them. Let us get started:

Let K be a filed.

Definition 6. *(1) An isomorphism σ of K with itself is called an automorphism of K. The collection of automorphisms of K is denoted* $\mathrm{Aut}(K)$. *If $\alpha \in K$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.*
(2) An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to fix an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is a subset of K (for example, a subfield), then an automorphism σ is said to fix F if it fixes all the elements of F, i.e., $\sigma a = a$ for all $a \in F$.

Nothing new here. Let us continue.

Definition 7. *Let K/F be an extension of fields. Let Aut (K/F) be the collection of automorphisms of K which fix F.*

I think some of you may ask: "You talked a lot about so-called Galois group, why here is automorphism group but not Galois group" . I want to make a clarification here. In fact, the Galois group is a special case of automorphism group. I will explain this in detail later. Since Galois makes a lot of contributions to the field theory, we use his name to name "good" things to distinguish from "bad" ones. For example, the normal separable extension is called Galois extension. The automorphism group of a Galois extension is called Galois group. And introduce the automorphism group of an extension of fields is just the learning order of "from general to special" .
And there is a important remark: Note that if F is the prime subfield of K then $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$ since every automorphism of K automatically fixes F. This is because the automorphism of field always fix 1 and the prime field is generated by 1 under $\{+, -, \times, \div\}$.

Proposition 8. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F), \sigma\alpha$ is a root of the minimal polynomial for α over F i.e., $\mathrm{Aut}(K/F)$ permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.*

You already proved this in our class. If you forget the proof please refer to the notes and try to remember it.

Example 9. $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq Z_2$, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \simeq \{e\}$.

证明. (1) Let $K = \mathbb{Q}(\sqrt{2})$. If $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\tau(\sqrt{2}) = \pm\sqrt{2}$ since these are the two roots of the minimal polynomial for $\sqrt{2}$. Since τ fixes $\mathbb{Q}$, this determines τ completely:

$$\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}.$$

The map $\sqrt{2} \mapsto \sqrt{2}$ is just the identity automorphism 1 of $\mathbb{Q}(\sqrt{2})$. The map $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ is the isomorphism (very easy to check it). Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ is a cyclic group of order 2 generated by σ.
(2) Let $K = \mathbb{Q}(\sqrt[3]{2})$. As before, if $\tau \in \mathrm{Aut}(K/\mathbb{Q})$, then τ is completely determined by its action on $\sqrt[3]{2}$ since

$$\tau\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) = a + b\tau\sqrt[3]{2} + c(\tau\sqrt[3]{2})^2$$

Since $\tau\sqrt[3]{2}$ must be a root of $x^3 - 2$ and the other two roots of this equation are not elements of K (recall the splitting field of this polynomial is degree 6 over $\mathbb{Q}$), the only possibility is $\tau\sqrt[3]{2} = \sqrt[3]{2}$ i.e., $\tau = 1$. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$ is the trivial group. □

Now we know that given a field extension K/F we can obtain a related group such as $\mathrm{Aut}(K/F)$. What about the reversed direction?

Proposition 10. *Let $H \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.*

Exercise 1. *Prove Proposition 10.*

证明. (OK, I know write the solution near the exercise is kind of "stupid" but I want to say, my purpose is not let you feel hard but let you know something. And I add "exercise" here is to remind you that you should know this proof).
Let $h \in H$ and let $a, b \in F$. Then by definition $h(a) = a, h(b) = b$ so that $h(a \pm b) = h(a) \pm h(b) = a \pm b, h(ab) = h(a)h(b) = ab$ and $h\left(a^{-1}\right) = h(a)^{-1} = a^{-1}$, so that F is closed, hence a subfield of K. □

Remark 11. *This proposition actually tell us for "general" field extension (in my words, both "good" ones and "bad" ones), the number of intermediate fields of K/F is at least the number of subgoups of $\mathrm{Aut}(K/F)$. If it is strictly more then this extension K/F is "bad" . So "good" means intermediate fields and subgroups has bijective correspondence, and we called a "good" field extension as Galois extension, call this correspondence Galois correspondence.*

Example 12. *("bad" example): Consider field extension $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{e\}$ only has one subgroup which is itself, but we have two fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}$ of this extension. If you want a "not very trivial" example, consider $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{e, \sigma\} \simeq Z_2$, it has no proper non-trivial subgroup but there exists non trivial intermediate fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.*

Definition 13. *If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all the elements of H is called the fixed field of H.*

Although general field extension is not always "good" , Galois extension. There are several things we should know and wo can prove them as some exercise.

Proposition 14. *The association of groups to fields and fields to groups defined above is inclusion reversing, namely,*
(1) if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\mathrm{Aut}\left(K/F_2\right) \leq \mathrm{Aut}\left(K/F_1\right)$, and
(2) if $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$.

Exercise 2. *Prove Proposition 14.*

证明. (1). $\forall \sigma \in \mathrm{Aut}\left(K/F_2\right)$, since σ fix F_2 pointwise and $F_1 \subset F_2$. Obviously σ fix F_1 pointwise. Thus $\sigma \in \mathrm{Aut}\left(K/F_1\right)$. And $\mathrm{Aut}\left(K/F_2\right)$ is actually a group so it is a subgroup of $\mathrm{Aut}\left(K/F_1\right)$.
(2). $\forall x \in F_2$, then $\forall \sigma \in H_2$, $\sigma x = x$. Since $H_1 \subset H_2$, $\forall \tau \in H_1$, $\tau x = x$. Thus $x \in F_1$. So $F_2 \subset F_1$. □

Now we have the intuiation that, "bad" extension means that the automorphisms is "not enough" . Or, the size of the automorphism group is "small" . How to make it as big as possible? Put all roots in it! And that is an informal description of the normal extension. Normal extension means, we add all roots of some polynomial to get a bigger field. It is enough for CharF=0 since we already know that every algebraic element over F is separable so finite normal extension is automatically Galois extension.

Theorem 15. *For any finite extension K/F, $|\mathrm{Aut}(K/F)| \leqslant [E : F]$*

We do not need to know the proof in our course since we never introduce character of groups over field. You can just assume this is true by our naive intuiation.

Definition 16. *Let K/F be a finite extension. Then K is said to be Galois over F and K/F is a Galois extension if $|\operatorname{Aut}(K/F)| = [K : F]$. If K/F is Galois the group of automorphisms Aut (K/F) is called the Galois group of K/F, denoted* $\operatorname{Gal}(K/F)$.

Corollary 17. *Let K/F be a finite extension with $CharF = 0$. Then K/F is Galois if and only if K is the splitting field of some polynomial over F.*

And finally I give the formal definition of Galois group of a polynomial:

Definition 18. *If $f(x)$ is a separable polynomial over F, then the Galois group of $f(x)$ over F is the Galois group of the splitting field of $f(x)$ over F.*

Also we still have a "formal" exercises which are left in our class, I list all of them here:

Exercise 3. *Prove that $f = x^5 - 6x + 3$, or $x^5 - 4x + 2$ are not soluble by radicals, i.e.* $\operatorname{Gal}(f)$ *is insoluble.*

证明. Hint: Use Proposition 4 in notes of Lecture 21. □