MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, March 31

Contractible spaces

Let Δ^n be the n-dimensional simplex (seen as a simplicial complex, i.e., including all of its subsimplices). We have $H_0(\Delta^n) = \mathbb{Z}$. One can show that $H_k(\Delta^n) = 0$ for all $k \geq 1$. In fact, homology can not distinguish Δ^n from the space consisting of a single point, since Δ^n is *contractible*. A space X is called *contractible* if there exists continuous map $f(x, t) : X \times [0, 1] \to X$ such that $f(x, 0) = x$ and $f(x, 1)$ is constant, i.e., if X can be continuously contracted to a point. Homology groups of any contractible space are the same as the homology group of a single point.

Brouwer fixed point theorem

Theorem 1

If $f : \Delta^n \to \Delta^n$ is continuous, then there exists $x \in \Delta^n$ such that $f(x) = x$. (I.e., f has a fixed point.)

(Prove it for $n = 1$!)

Suppose that it is not true, and let f be a continuous map without a fixed point. For every $x \in \Delta^n$ consider the ray from $f(x)$ to x, continue it to the intersection with the boundary of Δ^n. Let $g(x)$ be the point of intersection. Then $g : \Delta^n \to \partial\Delta^n$ is a continuous function. Consider the homomorphism $g_* : H_{n-1}(\Delta^n) \to H_{n-1}(\partial\Delta^n)$. But for every $y \in \partial\Delta^n$ we have $g(y) = y$, so the homology class of $\partial\Delta^n$ is mapped to the generator of the homology group $H_{n-1}(\partial\Delta^n) = \mathbb{Z}$. We get that 0 is mapped to a non-zero element, which is impossible.

Automorphisms of fields

Recall that an isomorphism of fields $\phi : F_1 \to F_2$ is a bijective map preserving the field operations, i.e., such that $\phi(a+b) = \phi(a) + \phi(b), \phi(ab) = \phi(a)\phi(b), \phi(a/b) = \phi(a)/\phi(b)$. In particular, $\phi(0) = 0$, $\phi(1) = 1$. Any homomorphism between fields is injective, and is an isomorphism with the image.
An isomorphism of a field with itself is called an *automorphism*.
Example: If F is a field of characteristic p, then $x \mapsto x^p$ is an automorphism of F. (Follows from the binomial formula.) It is called the *Frobenius automorphism*.

Theorem 2

Let $f(x) \in F[x]$ be an irreducible polynomial. Let E be an algebraic closure of F. Let $\alpha, \beta \in E$ be roots of $f(x)$. Then the map $\phi(\alpha) = \beta$, $\phi(x) = x$ for $x \in F$, extends to a unique isomorphism $F(\alpha) \to F(\beta)$.

The proof is recalling the fact, that both fields are isomorphic to $F[x]/(f)$ and the corresponding isomorphism maps x to α or β.

We say that $\alpha, \beta \in E$ are *conjugate* over F if they are roots of the same irreducible polynomial $f(x) \in F[x]$. Recall that for any element α algebraic over F there exists a unique irreducible polynomial $f(x)$ (up to multiplication by a constant) such that $f(\alpha) = 0$.

So, the last theorem can be reformulated as

Theorem 3

Two elements α, β algebraic over F are conjugate over F if and only if they are roots of the same irreducible polynomial over F.

For example, two complex numbers $z_1, z_2 \in \mathbb{C}$ are conjugate over $\mathbb{R}$ if and only if they are equal or conjugate (in the usual sense of complex conjugation), since irreducible polynomial of $a + ib$ is $x^2 - 2ax + (a^2 + b^2)$, which has roots $a + ib$ and $a - ib$.

Examples: the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$. Consequently, $a + b\sqrt{2}$ and $a - b\sqrt{2}$ are conjugate over $\mathbb{Q}$.

The map $\sqrt[3]{2} \mapsto \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ extends to an isomorphism $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}\left(\sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\right)$, and the elements $\sqrt[3]{2}$ and $\sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ are conjugate.

If σ is an automorphism of a field F, then its *fixed field* is the set of elements $x \in F$ such that $\sigma(x) = x$. Note that $\sigma(x) = x$ and $\sigma(y) = y$ imply $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$, $\sigma(x-y) = \sigma(x) - \sigma(y) = x - y$, $\sigma(xy) = \sigma(x)\sigma(y) = xy$, $\sigma(x/y) = \sigma(x)/\sigma(y) = x/y$. Consequently, the set of solutions of $\sigma(x) = x$ is a subfield of F.

For example, the fixed field of the complex conjugation is $\mathbb{R}$. The fixed field of the Frobenius automorphism is the set of roots of $z^p - z$, i.e., $\mathbb{Z}_p$.

More generally, we can consider a set of automorphisms S of F. Its *fixed field* F_S is the set of elements $x \in F$ such that $\sigma(x) = x$ for **every** $\sigma \in S$. Note that S will generate a group G, and if $x \in F_S$, then $x \in F_G$. So, it is natural to consider *groups of automorphisms* of F and their fixed fields.

Galois group

Recall that an *extension* of a field F is a field E such that $F \subset E$. We are interested in *automorphisms* of the extension, i.e., automorphisms $\phi : E \to E$ such that $\phi(x) = x$ for every $x \in F$. Note that such an automorphism is a linear map of the F-vector space E.

Example: complex conjugation is an automorphism of the extension $\mathbb{R} \subset \mathbb{C}$.

The *Galois group* $G(E/F)$ is the group of all automorphisms of the extension $F \subset E$, i.e., the group of all automorphisms of E fixing every element of F. We have then $F \subseteq E_{G(E/F)}$.

If G is a group of automorphisms of F, then we have $G \leq G(F/F_G)$. For every extension $F \subset E$ we have $F \subseteq E_{G(E/F)}$.
We will be interested in *intermediate subfields* $F \subseteq K \subseteq E$ of an extension $F \subseteq E$. If H is a subgroup of $G(E/F)$, then $F \subseteq E_H \subseteq E$. Conversely, if K is an intermediate subfield, then we can consider the subgroup $G(E/K) \leq G(E/F)$, (every automorphism fixing K also fixes F). We get two maps in two directions between the set of intermediate subfields and the set of subgroups of $G(E/F)$. One map transforms a subfield K into the subgroup $G(E/K)$. The other map transforms a subgroup H to the subfield E_H. Our goal is to describe a class of extensions for which these two maps are inverse to each other. Then we will get a bijection between the set of intermediate fields and the set of subgroups of $G(E/K)$. This will make it possible to study subfields using group theory.

An example.

Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We can write it as $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ or as $\mathbb{Q}(\sqrt{3})(\sqrt{2})$. It follows that there are automorphisms of $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ given by

$$\sigma_{\sqrt{2}}(\sqrt{2}) = -\sqrt{2}, \qquad \sigma_{\sqrt{2}}(\sqrt{3}) = \sqrt{3},$$

$$\sigma_{\sqrt{3}}(\sqrt{2}) = \sqrt{2}, \qquad \sigma_{\sqrt{3}}(\sqrt{3}) = -\sqrt{3}.$$

Their composition (in both orders) is the automorphism

$$\sqrt{2} \mapsto -\sqrt{2}, \qquad \sqrt{3} \mapsto -\sqrt{3}.$$

The group generated by $\sigma_{\sqrt{2}}$ and $\sigma_{\sqrt{3}}$ is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (i.e., the Klein's 4-group).

An example.

Note that minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, so any automorphism $g \in G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ must satisfy $g(\sqrt{2}) = \sqrt{2}$ or $g(\sqrt{2}) = -\sqrt{2}$. The same is true for $\sqrt{3}$. If you know $g(\sqrt{2})$ and $g(\sqrt{3})$ for $g \in G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, then you know g. It follows that we have found all elements of $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.
This group has three sub-groups of order two $\langle \sigma_{\sqrt{2}} \rangle$, $\langle \sigma_{\sqrt{3}} \rangle$, and $\langle \sigma_{\sqrt{2}} \sigma_{\sqrt{3}} \rangle$. There fixed fields are $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{6})$, respectively.
In this case the constructed maps between subfields and subgroups are bijections.