MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 16

	ϵ	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
$\alpha \mapsto$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$i \mapsto$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Let us see how they permute the roots.

$$\rho_1 : \alpha \mapsto i\alpha \mapsto i \cdot i\alpha = -\alpha \mapsto -i\alpha \mapsto -i(i\alpha) = \alpha$$

$$\rho_2 : \alpha \leftrightarrow -\alpha, \quad i\alpha \leftrightarrow -i\alpha$$

$$\rho_3 : \alpha \mapsto -i\alpha \mapsto -\alpha \mapsto i\alpha \mapsto \alpha$$

$$\mu_1 : \alpha \mapsto \alpha, -\alpha \mapsto -\alpha, i\alpha \leftrightarrow -i\alpha$$

$$\delta_1 : \alpha \mapsto i\alpha \mapsto (-i)(i\alpha) = \alpha, \quad -\alpha \leftrightarrow -i\alpha$$

$$\mu_2 : \alpha \leftrightarrow -\alpha, i\alpha \mapsto (-i)(-\alpha) = i\alpha, -i\alpha \mapsto -(-i)(-\alpha) = -i\alpha$$

$$\delta_2 : \alpha \mapsto -i\alpha, i\alpha \mapsto -i(-i\alpha) = -\alpha, -\alpha \mapsto i\alpha, -i\alpha \mapsto -(-i)(-i\alpha) = -\alpha$$

We see that it acts as D_4 on the square of roots of $x^4 - 2$.

The group D_4 has one cyclic subgroup of order 4: $\{\epsilon, \rho_1, \rho_2, \rho_3\}$ two subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (generated reflections with respect to the two diagonals and generated by reflections with respect to two lines parallel to the sides): $\{\epsilon, \mu_1, \mu_2, \rho_2\}$ and $\{\epsilon, \delta_1, \delta_2, \rho_2\}$. Each of the elements of order 2 $\{\rho_2, \mu_1, \mu_2, \delta_1, \delta_2\}$ generates a subgroup of order 2. And then there is the trivial subgroup and the whole group.

Let us find the fixed fields of the subgroups. The field corresponding to groups of order 4 must be a quadratic extension of $\mathbb{Q}$, since the index of the subgroup is 2. We have i, $\sqrt{2}$, and $i\sqrt{2}$ in the field. Note that $\rho_1(i) = i$, so i belongs to the fixed field of the cyclic group generated by ρ_1. It follows that the fixed field of the cyclic group is $\mathbb{Q}(i)$. We have $\mu_1(\sqrt{2}) = \mu_1(\alpha^2) = \alpha^2$ and $\mu_2(\sqrt{2}) = \mu_2(\alpha^2) = (-\alpha)^2 = \alpha^2$, hence $\mathbb{Q}(\sqrt{2})$ is in the fixed field of $\{\epsilon, \mu_1, \mu_2, \rho_2\}$. Similarly, $\delta_1(i\sqrt{2}) = \delta_1(i\alpha^2) = -i(i\alpha)^2 = i\alpha^2$ and $\delta_2(i\sqrt{2}) = -i(-i\alpha)^2 = i\alpha^2$, hence the fixed field of $\{\epsilon, \delta_1, \delta_2, \rho_2\}$ is $\mathbb{Q}(i\sqrt{2})$.

It remains to find the fixed fields of groups of order two. They must be degree 4 extensions of $\mathbb{Q}$. ρ_2 fixes i and $\alpha^2 = \sqrt{2}$, which gives the degree 4 extension $\mathbb{Q}(i, \sqrt{2})$. μ_1 fixes $\sqrt[4]{2}$, which $\mathbb{Q}(\sqrt[4]{2})$. μ_2 fixes $i\sqrt[4]{2}$, so it gives $\mathbb{Q}(i\sqrt[4]{2})$. δ_1 switches α with $i\alpha$, so it leaves $\alpha + i\alpha$ fixed, so it gives $\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$. δ_2 switches α and $-i\alpha$, and we get $\mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$.

Cyclotomic extensions

The splitting field of $x^n - 1$ over F is the *nth cyclotomic extension of* F. If α is a root of $x^n - 1$, then using long division, we get $g(x) = \frac{x^n-1}{x-\alpha} = x^{n-1} + \alpha x^{n-2} + \alpha^2 x^{n-3} + \cdots + \alpha^{n-2}x + \alpha^{n-1}$, hence $g(\alpha) = n\alpha^{n-1} = n\alpha^{-1}$. This is not equal to zero if and only if n is not divisible by the characteristic of F. Consequently, if n is not divisible by the characteristic, then all roots of $x^n - 1$ are simple, and the cyclotomic extension is separable.

The set of roots α of $x^n - 1$ is a group with respect to multiplication. Since it is a subgroup of the multiplicative group of a field, it is cyclic. Hence it is isomorphic to $\mathbb{Z}_n$. Recall that a residue k modulo n is a generator of $\mathbb{Z}_n$ if and only if n and k are coprime. It follows that the group of roots of $x^n - 1$ has $\phi(n)$ generating elements. They are called the *primitive roots*. Since the property of being primitive is purely algebraic, any automorphism of the cyclotomic field must map a primitive root to a primitive root. It follows that the product of all $(x - \alpha)$ for primitive roots α is a polynomial invariant under the action of the automorphism group of the cyclotomic extension, hence all its coefficients belong to the simple subfield of F (i.e., to $\mathbb{Z}_p$ for fields of characteristic p and to $\mathbb{Q}$ for fields of 0 characteristic). We denote this polynomial by $\Phi_n(x)$. We know that $\deg \Phi_n = \phi(n)$.

Since a root is primitive if and only if it does not generate a smaller subgroup, it is primitive if and only if it is not a root of $x^k - 1$ for some $k < n$. It follows that

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}.$$

This gives another proof that $\Phi_n(x) \in \mathbb{Z}[x]$. For example, we have $\Phi_1(x) = x - 1$, $\Phi_2(x) = \frac{x^2-1}{x-1} = x + 1$, $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$, $\Phi_4(x) = \frac{x^4-1}{x^2-1} = x^2 + 1$, $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ if p is prime, $\Phi_6(x) = \frac{x^6-1}{(x^3-1)(x+1)} = x^2 - x + 1$. They are called *cyclotomic polynomials*.