

# Dedekind's Theorem on Galois Groups and Chebotarev's Density Theorem

Timo Chang

[timo65537@protonmail.com](mailto:timo65537@protonmail.com)

Last edited: November 7, 2024

Given an irreducible polynomial  $f(x) \in \mathbb{Q}[x]$ . Let  $K$  be the splitting field of  $f(x)$  over  $\mathbb{Q}$ . One can ask how to determine the Galois group  $\text{Gal}(f) := \text{Gal}(K/\mathbb{Q})$ . In the first half of the essay, we prove a theorem due to Dedekind, which describes certain elements in  $\text{Gal}(f)$ , and thereby giving some limitations on the structure of  $\text{Gal}(f)$ . Next, we mention a striking result due to Chebotarev, called Chebotarev's density theorem.

## 1 Dedekind's theorem on Galois groups

**Theorem 1.1** (Dedekind). *Suppose  $f(x) \in \mathbb{Z}[x]$  is monic and irreducible. For each prime number  $p$  not dividing  $\text{disc}(f)$ , write  $f(x) = f_1(x) \cdots f_k(x)$  in  $(\mathbb{Z}/p\mathbb{Z})[x]$  where each  $f_i(x)$  is irreducible. Assume  $\deg f_i = d_i$ . Then  $\text{Gal}(f)$  has an element which permutes the roots of  $f(x)$  with cycle type  $(d_1, \dots, d_k)$ .*

For simplicity we will say that  $p$  “gives” the cycle type  $(d_1, \dots, d_k)$ , and  $\text{Gal}(f)$  has an element with cycle type  $(d_1, \dots, d_k)$ .

This theorem can be explained very quickly from algebraic number theory. Basically,  $p \nmid \text{disc}(f)$  implies that  $p$  is unramified in  $K$ . And the element we're looking for is just an (any) element in the Artin conjugacy class of  $p$  (see Remark 1.2 also). Let's make this precise.

*Proof.* Let  $\alpha$  be any root of  $f(x)$  in  $K$  and  $E := \mathbb{Q}(\alpha)$ . As  $p \nmid \text{disc}(f)$ , we know  $p \nmid \text{disc}(E)$  and so  $p$  is unramified in  $E$ . As  $K$  is the field extension of  $\mathbb{Q}$  joining all conjugates of  $\alpha$  (i.e., all roots of  $f(x)$ ), we have  $p$  is unramified in  $K$ .

Take a prime  $P$  in  $K$  lying over  $p$ . As  $P/p$  is unramified, the decomposition group  $D(P/p)$  is isomorphic to the Galois group of the residue field extension  $\mathcal{O}_K/P$  over  $\mathbb{Z}/p\mathbb{Z}$ . The latter is a cyclic group generated by the Frobenius automorphism  $\sigma_p$ , which sends an element in  $\mathcal{O}_K/P$  to its  $p$ -th power. We let  $\phi := \phi(P/p)$  be the corresponding element in  $D(P/p) \subseteq \text{Gal}(K/\mathbb{Q})$ , which is characterized by the condition  $\phi(\alpha) \equiv \alpha^p \pmod{P}$  for all

$\alpha \in \mathcal{O}_K$ . (In other words, we have  $\overline{\phi(\alpha)} = \overline{\alpha^p}$  in  $\mathcal{O}_K/P$ .) We claim that  $\phi$  has the desired cycle type.

Write  $f(x) = f_1(x) \cdots f_k(x)$  into irreducible factors in  $(\mathbb{Z}/p\mathbb{Z})[x]$  where  $\deg f_i = d_i$ . As  $p \nmid \text{disc}(f)$ , all the roots of  $f(x)$  are distinct modulo  $P$ . Now, for each  $i = 1, \dots, k$ , pick a root  $\overline{\alpha_i}$  of  $f_i(x)$ . Note that the Frobenius automorphism  $\sigma_p$  generates all the conjugates of  $\overline{\alpha_i}$ . That is to say, the roots of  $f_i(x)$  are given by

$$\{\overline{\alpha_i}, \overline{\alpha_i^p}, \dots, \overline{\alpha_i^{p^{d_i-1}}}\} = \{\overline{\alpha_i}, \overline{\phi(\alpha_i)}, \dots, \overline{\phi^{d_i-1}(\alpha_i)}\} \quad \text{and} \quad \overline{\alpha_i^{p^{d_i}}} = \overline{\phi^{d_i}(\alpha_i)} = \overline{\alpha_i}.$$

Translating back to  $f(x)$ , this means the element  $\phi$  acts as a  $d_i$ -cycle on the roots of  $f(x)$  which correspond to the roots of  $f_i(x)$ . This completes the proof.  $\square$

*Remark 1.2.* Since different primes  $P$  in  $K$  lying over  $p$  correspond to different  $\phi(P/p)$  up to conjugation, these elements are actually in the same conjugacy class of  $\text{Gal}(f)$ , called the *Artin conjugacy class of  $p$* . In particular, they have the same cycle type. Hence, the cycle type is independent of the choices of  $P$  over  $p$ . This justifies the saying that  $p$  (not  $P/p$ ) gives the cycle type  $(d_1, \dots, d_k)$ .

Before we compute some examples, let us first recall the determination of quartic Galois groups. Suppose  $f(x) \in \mathbb{Q}[x]$  is irreducible of degree 4. Let  $R_3(f)$  be the cubic resolvent of  $f$ . Then we have

$\text{disc}(f)$	$R_3(f)$	$\text{Gal}(f)$
= square in $\mathbb{Q}$	irreducible	$A_4$
= square in $\mathbb{Q}$	not irreducible	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\neq$ square in $\mathbb{Q}$	irreducible	$S_4$
$\neq$ square in $\mathbb{Q}$	not irreducible	$D_4$ or $\mathbb{Z}/4\mathbb{Z}$ .

We also note that the differentiation between  $D_4$  and  $\mathbb{Z}/4\mathbb{Z}$  is rather technical and not straightforward. (For a complete material on this topic, see [Con].)

**Example 1.3.** Consider the irreducible polynomial  $f(x) = x^4 + x - 1$ . Note that  $\text{disc}(f) = -283$ , which is not a square in  $\mathbb{Q}$ . So  $\text{Gal}(f) = S_4, D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ . Moreover, the cubic resolvent of  $f$  is  $R_3(f) = x^3 + 4x - 1$ , which is irreducible. So we conclude that  $\text{Gal}(f) = S_4$ .

We can also use Theorem 1.1 instead of the cubic resolvent. Note that the discriminant of  $f$  is (luckily) a prime. So we may pick some small prime numbers  $p$  and consider the factorization of  $f(x)$  in  $(\mathbb{Z}/p\mathbb{Z})[x]$ . Again, as  $\text{disc}(f) = -283$  is not a square in  $\mathbb{Q}$ , we know  $\text{Gal}(f) = S_4, D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ .

- $p = 2$ .  $f(x) = x^4 + x + 1$  in  $(\mathbb{Z}/2\mathbb{Z})[x]$ . So  $\text{Gal}(f)$  has an element of cycle type (4).  
But this doesn't help because all three remaining possibilities contain such element.
- $p = 3$ .  $f(x) = x^4 + x + 2$  in  $(\mathbb{Z}/3\mathbb{Z})[x] \implies$  no conclusion.

- $p = 5$ .  $f(x) = x^4 + x + 4$  in  $(\mathbb{Z}/5\mathbb{Z})[x] \implies$  no conclusion.
- $p = 7$ .  $f(x) = (x + 3)(x^3 + 4x^2 + 2x + 2)$  in  $(\mathbb{Z}/7\mathbb{Z})[x]$ . So  $\text{Gal}(f)$  has an element of cycle type  $(1, 3)$ . This eliminates  $D_4$  and  $\mathbb{Z}/4\mathbb{Z}$ .

We may now conclude that  $\text{Gal}(f) = S_4$ .

**Example 1.4.** Consider the irreducible polynomial  $f(x) = x^4 - 2x^2 + 7$ . Note that  $\text{disc}(f) = 2^{10} \cdot 3^2 \cdot 7$ , which is not a square in  $\mathbb{Q}$ . So  $\text{Gal}(f) = S_4, D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ . Moreover, the cubic resolvent of  $f$  is  $R_3(f) = x^3 + 2x^2 - 28x - 56 = (x + 2)(x^2 - 28)$ , which is reducible. So  $\text{Gal}(f) = D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ .

To apply Theorem 1.1, we can only consider primes not dividing  $\text{disc}(f)$ . So we start at  $p = 5$ . Note  $f(x) = (x + 2)(x + 3)(x^2 + 2)$  in  $(\mathbb{Z}/5\mathbb{Z})[x]$ . So  $\text{Gal}(f)$  has an element of cycle type  $(1, 1, 2)$ . This eliminates  $\mathbb{Z}/4\mathbb{Z}$ . So we conclude that  $\text{Gal}(f) = D_4$ .

**Example 1.5.** Let's consider an example of quintic polynomial. Say  $f(x) = x^5 - x - 1$ , irreducible with  $\text{disc}(f) = 19 \cdot 151$ . First of all, since we're considering quintic polynomial, so we must have  $5 \mid \#(\text{Gal}(f))$  and  $\#(\text{Gal}(f)) \mid 5! = 120$  as the Galois group embeds into  $S_5$ .

Next, we pick  $p = 2 \nmid \text{disc}(f)$  and see that  $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$  in  $(\mathbb{Z}/2\mathbb{Z})[x]$ . So  $\text{Gal}(f)$  has an element of cycle type  $(2, 3)$ . In particular,  $\text{Gal}(f)$  has an element of order 6, which implies  $6 \mid \#(\text{Gal}(f))$ . This together with the first observation force  $\#(\text{Gal}(f)) = 30, 60, 120$ .

Note that 30 is impossible because  $S_5$  has no subgroup of order 30 (why?). And since  $\text{disc}(f)$  is not a square in  $\mathbb{Q}$ , so  $\text{Gal}(f)$  is not contained in  $A_5$ . In particular,  $\#(\text{Gal}(f)) \neq 60$ . Hence, we may conclude that  $\text{Gal}(f) = S_5$ .

**Example 1.6.** Finally, we consider the quartic irreducible polynomial  $f(x) = x^4 + 5x + 5$  with  $\text{disc}(f) = 5^3 \cdot 11^2$ . A similar procedure as in Example 1.4 shows that  $\text{Gal}(f) = D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ . We then try to apply Theorem 1.1. But after a little trial and error, one sees that no conclusion can be drawn for small prime numbers. It then makes you wonder whether such a “useful” prime exists.

It turns out that, it doesn't. Further analysis (see [Con]) shows that  $\text{Gal}(f) = \mathbb{Z}/4\mathbb{Z}$ . So no matter how far we go, we'll only be able to get cycle types  $(4), (2, 2)$  and  $(1, 1, 1, 1)$ . But  $D_4$  also contains these three cycle types. So it is impossible to eliminate  $D_4$  by the previous strategy.

A natural question arises from Example 1.6: What prime numbers give a certain cycle type. Or perhaps with less ambition, how many prime numbers give a certain cycle type. The latter is answered by Chebotarev's density theorem, which concerns the “distributive behavior” of those unramified primes. (This may in some sense help us find  $\text{Gal}(f)$ .)

## 2 Chebotarev's Density Theorem

Let us first make some numerical observations via Example 1.3 and 1.4. Searching out the first 10000 prime numbers not dividing  $\text{disc}(f)$ , we obtain the following table indicating how many of them give the certain cycle types.

$f(x)$	$\text{Gal}(f)$	(4)	(1, 3)	(2, 2)	(1, 1, 2)	(1, 1, 1, 1)
$x^4 + x - 1$	$S_4$	2496	3322	1244	2545	393
$x^4 - 2x^2 + 7$	$D_4$	2520	0	3738	2508	1234

Notice that the ratios are very close to

$f(x)$	$\text{Gal}(f)$	(4)	(1, 3)	(2, 2)	(1, 1, 2)	(1, 1, 1, 1)
$x^4 + x - 1$	$S_4$	1/4	1/3	1/8	1/4	1/24
$x^4 - 2x^2 + 7$	$D_4$	1/4	0	3/8	1/4	1/8

It turns out that, these distributive results are measured by the “size” of the conjugacy classes in  $\text{Gal}(f)$ . Precisely, we have the following.

**Theorem 2.1** (Chebotarev's Density Theorem). *Let  $L/K$  be a finite Galois extension of number fields with Galois group  $G$ . Let  $C \subseteq G$  be a conjugacy class. Then the set  $M_C$  of primes  $\mathfrak{p}$  of  $K$  which are unramified in  $L$  and for which there exists a prime  $\mathfrak{P}$  of  $L$  lying above  $\mathfrak{p}$  such that the Frobenius automorphism  $\phi(\mathfrak{P}/\mathfrak{p}) \in C$  has (natural) density  $\#(C)/\#(G)$ . In other words,*

$$\lim_{n \rightarrow \infty} \frac{\#\{\mathfrak{p} \in M_C \text{ with } N\mathfrak{p} \leq n\}}{\#\{\mathfrak{p} \text{ with } N\mathfrak{p} \leq n\}} = \frac{\#(C)}{\#(G)}.$$

Now, we apply Chebotarev's density theorem to the settings of Dedekind's theorem. Suppose we're given a conjugacy class  $C \subseteq \text{Gal}(f)$  whose elements have cycle type  $(d_1, \dots, d_k)$ . Then from the proof of Theorem 1.1, we see that  $p$  gives this cycle type if and only if the element  $\phi(P/p) \in C$  for some prime  $P$  over  $p$ . And this by definition is equivalent to  $p \in M_C$ . So asking how many prime numbers give a certain cycle type is equivalent to asking how “large” is the set  $M_C$ . And the latter is answered by Theorem 2.1. This helps us explain our numerical data.

Say  $f(x) = x^4 + x - 1$  with  $\text{Gal}(f) = S_4$ . Consider the conjugacy class  $C$  whose elements have cycle type (4). One sees that  $\#(C) = 6$ . So by Theorem 2.1, the primes which give the cycle type (4) has density  $\#(C)/\#(G) = 6/24 = 1/4$ . This matches our numerical experiment.

On the other hand, say  $f(x) = x^4 - 2x^2 + 7$  with  $\text{Gal}(f) = D_4$ . Note that no first 10000 primes not dividing  $\text{disc}(f)$  gives the cycle type (1, 3). This should really be expected because  $D_4$  contains no element with cycle type (1, 3).

We can also guess the Galois group based on the numerical data. In Example 1.6 we saw that Dedekind's theorem fails to work directly for the polynomial  $f(x) = x^4 + 5x + 5$ . But we can still do the same computation and get the table

$f(x)$	$\text{Gal}(f)$	(4)	(1, 3)	(2, 2)	(1, 1, 2)	(1, 1, 1, 1)
$x^4 + 5x + 5$	?	5025	0	2492	0	2483

Since  $\text{disc}(f) = 5^3 \cdot 11^2$  is not a square in  $\mathbb{Q}$ . So  $\text{Gal}(f) = S_4, D_4$  or  $\mathbb{Z}/4\mathbb{Z}$ . Moreover, the cycle type (1, 1, 1, 1) (which corresponds to the conjugacy class consisting of only the identity element) appears with frequency  $2483/10000 \approx 1/4$ . And by Theorem 2.1, this number should be close  $1/\#(G)$ . So we may guess  $\#(G) = 4$  and  $G = \mathbb{Z}/4\mathbb{Z}$ . This is indeed the case. (But certainly, this is not a proof.)

## References

- [Con] Keith Conrad. "Galois groups of cubics and quartics (not in characteristic 2)". In: *Expository papers* ().