

# NORI'S ALGEBRAIC NUMBER

THEORY LECTURES — SUMMER 2007

Lecture 9: 07/19/2007

## §9.1. Weber Class Group.

$K$  = number field

$\mathcal{O}(K)$  = ring of integers in  $K$

$C \subset \mathcal{O}(K)$  an ideal  $\Rightarrow C = \prod_{i=1}^k P_i^{m_i}$

with  $m_i \in \mathbb{N}$ ,  $P_i \subset \mathcal{O}(K)$  distinct maximal ideals

$\mathcal{L}_C = \left\{ I \subset K \mid \begin{array}{l} I \text{ is a fractional ideal} \\ \text{and } I_{P_i} = \mathcal{O}(K)_{P_i} \text{ for} \\ \text{all } 1 \leq i \leq k \end{array} \right\}$

This is a group under multiplication which depends only on the radical of  $C$ .

Further, we define

$R = \bigcap_{i=1}^k \mathcal{O}(K)_{P_i}$  a semi-local ring

$T(C) = \left\{ \alpha \in R \mid \alpha \equiv 1 \pmod{CR} \right\}$

↑  
extension of  $C$  to an ideal of  $R$

§9.2. Definition. The Weber class group associated to  $C$  is defined by

$$\mathcal{L}_C / \{ \mathcal{O}(K)^\times \mid \alpha \in T(C) \}$$

Example.  $K = \mathbb{Q}$ ;  $C = n\mathbb{Z}$ ,

where  $n$  is a natural number.

Check that the Weber class group in this case is  $\cong (\mathbb{Z}/n\mathbb{Z})^\times$ .

§9.3. Consider a Galois extension  $L/K$  of number fields. Write

$$S = \left\{ v \in \Sigma_f(K) \mid \left. \begin{array}{l} \text{for some } w \mid v, \\ L_w \text{ is ramified} \\ \text{over } K_w \end{array} \right\} \right\}$$

Remarks: (a) ramified := not unramified;  
(b) since  $L/K$  is Galois, "for some"  $\Leftrightarrow$  "for all" in the above definition, but in general, "for some" is the correct version

For any  $v \in \Sigma_f(K) \setminus S$ , we have a well defined conjugacy class  $\langle \text{Frob}_v \rangle \subset \text{Gal}(L/K)$ .

We have proved last time that  $S$  is a finite set.

### §9.4. Chebotarev density theorem.

Fix a conjugacy class  $X \subset G$ .

Write  $F_X = \{v \in \Sigma_f(K) \setminus S \mid \langle \text{Frob}_v \rangle = X\}$ .

This set is infinite; in fact, it has positive density in the following sense.

For each  $N \in \mathbb{N}$ , write

$$A_N = \#\{v \in \Sigma_f(K) \mid |k_v| \leq N\} \text{ and}$$

$$B_N = \#\left\{v \in \Sigma_f(K) \setminus S \mid \begin{array}{l} |k_v| \leq N \\ \text{and} \\ \langle \text{Frob}_v \rangle = X \end{array}\right\}.$$

$$\text{Then } \lim_{N \rightarrow \infty} \frac{B_N}{A_N} = \frac{\#X}{\#G}.$$

§9.5. Example. (Dirichlet density is a special case of Chebotarev density.)

Consider  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(\zeta_n)$ ,

where  $\zeta_n$  is a primitive  $n$ -th root of 1 and  $n \in \mathbb{N}$ . Then, as we saw before,

$$S = \{p = \text{rational prime} \mid p \mid n\}.$$

$$\text{We have } \text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

If  $p$  is a rational prime,  $p \notin S$ , then  $\text{Frob}_p = p \pmod n$ .

4

Hence we see that for any  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ , the density of the set of rational primes  $p$  with  $p \equiv a \pmod{n}$  is equal to  $\frac{1}{\varphi(n)}$ , where  $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ .

**§9.6. Exercise.** Fix a number field  $K$ .

Given any finite set  $S$  of nonzero prime ideals in  $\mathcal{O}(K)$ , write

$$F(S) = \text{g.c.d.} \left\{ \#(\mathcal{O}(K)/Q)^\times \mid Q \notin S \right\}$$

Note that  $S_1 \subset S_2 \Rightarrow F(S_1) \mid F(S_2)$ .

(a) Show that there exist  $N \in \mathbb{N}$  and a finite set  $S_0$  of nonzero prime ideals of  $\mathcal{O}(K)$  such that

$$S' \supset S_0 \Rightarrow F(S') = N$$

(b) Also, show that  $N$  is the number of roots of unity contained in  $K$ .

(Nori does not know of any purely algebraic proof of statement (b).)

**§9.7.** From now on,  $L/K$  is an

abelian Galois extension of number fields. Let  $G = \text{Gal}(L/K)$ , and let  $S_0 \subset \Sigma_f(K)$  denote the set of ramified primes, as before.

Let  $S \subset \Sigma_f(K)$  be any finite subset which contains  $S_0$ . Since  $G$  is commutative, for any  $v \in \Sigma_f(K) \setminus S$ , we get a well defined element  $\text{Frob}_v \in G$ . This extends to a surjective homomorphism

$$\mathbb{Z}[\Sigma_f(K) \setminus S] \longrightarrow G$$

||  
 group of fractional ideals on  $K$  which are relatively prime to  $S$ .  
 This homomorphism is called the Artin symbol.

**§9.8.** Weak form of Artin reciprocity.

There exists a nonzero ideal  $C \subset \mathcal{O}(K)$ ,

$$C = \prod_{i=1}^r P_i^{m_i} \quad (m_i \in \mathbb{N}), \text{ so that}$$

$$\{P_1, \dots, P_r\} = \{\text{ramified primes}\}$$

and so that the Artin symbol factors through the Weber class group for the ideal  $C$ .

Remark. Lang's algebraic number theory book explains how to compute  $C$  explicitly.

Example.  $K = \mathbb{Q}$        $L = \mathbb{Q}(\zeta_n)$   
 $C = n\mathbb{Z}$       and the result above holds

### §9.9. Principles.

- ① If Artin reciprocity holds for  $L/K$  and  $E$  is a finite extension of  $K$ , then Artin reciprocity also holds for  $LE/KE$ .
- ② If  $L \supset L' \supset K$  and A. r. l. holds for  $L/K$ , then it holds for  $L'/K$ .

§9.10. We will apply the second principle to the cubic reciprocity law.

From now on,  $K = \mathbb{Q}(\omega)$ , where  $\omega$  is a primitive cube root of unity. Take  $\alpha \in K$  which does not have a cube root in  $K$ , and put  $L = K(\alpha^{1/3})$ . Clearly,  $L$  is an abelian Galois extension of  $K$  (because  $\omega \in K$ ), and

$$\text{Gal}(L'/K) \xrightarrow{\cong} \mu_3(K)$$
$$\sigma \longmapsto \sigma(\alpha^{1/3}) / \alpha^{1/3}$$

Let  $\mathfrak{p} \subset \mathcal{O}(K)$  be any nonzero prime ideal such that  $\text{char}(\mathcal{O}(K)/\mathfrak{p}) \neq 3$ .

Let  $\alpha \in K$  be coprime to  $\mathfrak{p}$ , i.e.,  $\alpha$  is a unit of the localization  $\mathcal{O}(K)_{\mathfrak{p}}$ .

§ In this situation, we will define the symbol  $\left(\frac{\alpha}{P}\right) \in \mu_3(K)$ .

Now  $P$  is unramified in  $L'$ , so we have  $\sigma := \text{Frob}_P$ . Then

$$\sigma(\alpha^{1/3}) \equiv (\alpha^{1/3})^q \equiv \alpha^{1/3} \cdot \alpha^{\frac{q-1}{3}}$$

modulo some  $P' \subset \mathcal{O}(L')$  such that  $P' \cap \mathcal{O}(K) = P$ .

Here,  $q = \#(\mathcal{O}(K)/P)$ . Note that  $q-1$  is divisible by 3 because  $\mathbb{F}_q$  contains all cube roots of unity, by construction.

Def:  $\left(\frac{\alpha}{P}\right) \equiv \alpha^{\frac{q-1}{3}} \pmod{P}$ .

§9.11. Now consider  $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ , where  $p$  is a prime,  $p \equiv 1 \pmod{3}$ .

Put  $L = \mathbb{K}(\zeta_p) = \mathbb{Q}(\omega, \zeta_p)$ . Then  $L/\mathbb{K}$  is cyclic of degree  $p-1$ , and since  $3 \mid (p-1)$ ,  $L$  contains  $L'$  as above (for some  $\alpha \in \mathbb{K}$ ). So for all such  $\alpha$ 's we can get a reciprocity statement; however, not all  $\alpha$ 's occur in this way!

Then the game will be to deduce a reciprocity law for all other  $d > 5$ .

**§9.12.** Let us first identify  $L'$ .

We have  $\text{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

$$\sigma_c \longleftarrow c$$

↑ notation

Choose  $\chi: (\mathbb{Z}/p\mathbb{Z})^{\times} \longrightarrow \mu_3(K)$

Take any  $\alpha \in L$ , and consider

$$\beta := \sum_{c=1}^{p-1} \chi(c)^{-1} \sigma_c(\alpha)$$

Then, by construction,

$$\sigma_c(\beta) = \chi(c) \cdot \beta \quad \forall c \in (\mathbb{Z}/p\mathbb{Z})^{\times}$$

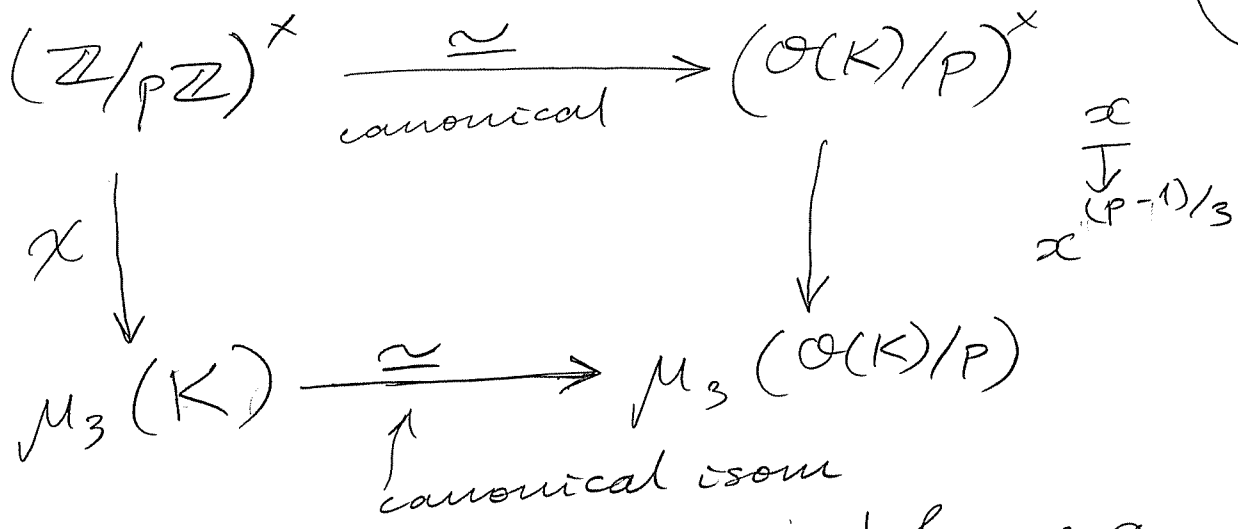
Thus  $\beta \in L' := L^{\text{Ker}(\chi)}$ , and also  $\beta^3 \in K$ .

**§9.13.** Special case:  $\alpha = \sum_p =: \sum$

Then  $\beta = \sum \chi$ , a Gaussian sum.

We would like to understand the prime factorization of  $\sum \chi^3 \in K$ .

Fix a prime ideal  $P \subset \mathcal{O}(K)$  such that  $P \cap \mathbb{Z} = (p)$ . Then  $\#(\mathcal{O}(K)/P) = p$ , so  $(p) = P \cdot \bar{P}$ , where  $\bar{P}$  is the complex conjugate of  $P$ .



This commutative diagram defines a natural choice of  $\chi$ , depending on  $\mathfrak{p}$ .

**§9.14. Proposition 1.**

$$\sum_{\chi}^3 \chi(\mathfrak{p}) = \mathfrak{p} \cdot \overline{\mathfrak{p}}^2$$

**Proposition 2.**

$$\sum_{\chi}^3 \chi \equiv -1 \pmod{3}.$$

Let us assume these two results for the moment, and see what happens when we apply Principle 9.9.2 to the extensions  $K \subset L' \subset L$  we constructed.

**§9.15.**

Let  $\mathfrak{Q}$  be any prime ideal of  $\mathcal{O}(K)$  with  $\text{char } k_{\mathfrak{Q}} \neq 3, p$ ; write  $q = \# k_{\mathfrak{Q}}$ .

$$\begin{aligned}
 \text{Then } \text{Frob}_{\mathfrak{Q}}(L/K) &= \sigma_q \\
 \Rightarrow \text{Frob}_{\mathfrak{Q}}(L'/K) &= \chi(q)
 \end{aligned}$$

Let  $\theta = \sum_{\chi}^3 \chi$ ; it follows that  $\left(\frac{\theta}{\mathfrak{Q}}\right) = \chi(q)$ .  
 By definition,  $\chi(q) \equiv q^{\frac{p-1}{3}} \pmod{p}$ .

Hence we get

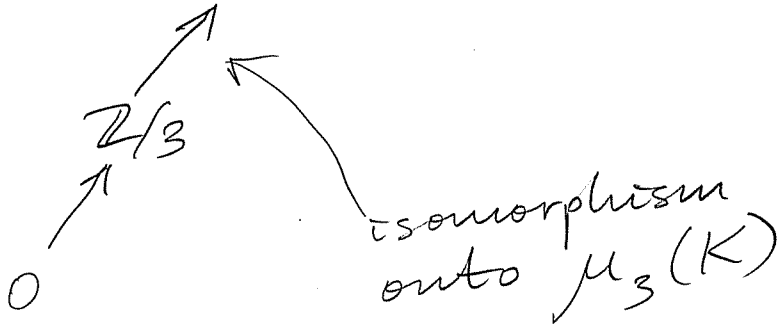
$$\left(\frac{\theta}{Q}\right) = \left(\frac{q}{P}\right) = \left(\frac{Q\bar{Q}}{P}\right)$$

**§9.16.** Remark.

$$\left(\frac{\theta(K)}{(3)}\right)^x \longrightarrow \left(\frac{\theta(K)}{(\omega-1)}\right)^x \longrightarrow 0$$

$$\parallel$$

$$\left(\frac{\mathbb{Z}}{3}\right)^x = \{\pm 1\}$$



In other words:  $\mu_3(K) \cong (1+I)/(1+I^2)$ ,  
where  $I = (1-\omega)$ .

Thus every ideal  $J \subset \mathcal{O}(K)$  which is coprime to  $(3)$ , i.e.,  $J+(3) = \mathcal{O}(K)$ , has a unique generator  $j$  with  $j \equiv 1 \pmod{3}$ .

**§9.17.** We work with  $\alpha \in \mathcal{O}(K)$  s.t.  $\alpha \equiv 1 \pmod{3}$ .  
Then  $\left(\frac{\alpha}{Q}\right) \stackrel{\text{def}}{=} \left(\frac{\mathcal{O}_K \alpha}{Q}\right)$  is well defined.

From the formula above, we obtain

$$\left(\frac{P\bar{P}^2}{Q}\right) = \left(\frac{Q\bar{Q}}{P}\right), \quad (9.17.1)$$

under the given hypotheses:  $\text{char } k_P$ ,  $\text{char } k_Q$ ,  $3$  all pairwise distinct and  $\text{char}(k_P) \equiv 1 \pmod{3}$ .

We claim that the following also holds: (11)

$$\left(\frac{Q\bar{Q}^2}{P}\right) = \left(\frac{P\bar{P}}{Q}\right) \quad (9.17.2)$$

under the same assumptions. Indeed, if  $Q = m\mathbb{Z}[\omega]$  with  $m = \text{prime} \equiv 2 \pmod{3}$ , one can easily check that both sides of (9.17.2) are equal to 1.

**§9.18.** Combining (9.17.1) and (9.17.2),

we obtain 
$$\left(\frac{\bar{P}}{Q}\right) \left(\frac{\bar{Q}}{P}\right) = 1.$$

Replacing  $P$  by  $\bar{P}$ , we get

$$\left(\frac{P}{Q}\right) \left(\frac{\bar{Q}}{\bar{P}}\right) = 1.$$

Finally, this implies

$$\boxed{\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)}$$

This is most of the reciprocity law...

**§9.19.** Sketch of proof of Proposition 9.14.1.

First show that  $|\mathcal{S}_x| = \sqrt{p}$ .

Hence  $|\mathcal{S}_x^3| = p^{3/2}$  under all complex embeddings

(This is a simple computation.)

This implies that  $\sum_x^3 O(K) = P^i \bar{P}^j$ , (12)  
and we only need to find out what  
 $i$  and  $j$  are... (the rest is omitted)  
( $i+j=3$ )