

## Lecture 9

We continue our discussion of the units in the ring of integers  $A$  of a number field  $k$ .

**Corollary 46.** (Kronecker) *If  $\epsilon$  is an algebraic integer such that  $|\epsilon|_v = 1$  for all infinite valuations  $v$ , then  $\epsilon$  is a root of unity.*

*Proof.* Since  $|\mathbb{N}(\epsilon)| = \prod_{v|\infty} |\epsilon|_v = 1$ , Corollary 41 implies that  $\epsilon$  is a unit in  $A$ . Letting  $\lambda : A^\times \rightarrow \bigoplus_{v|\infty} \mathbb{R}v$  be given by  $\alpha \mapsto \sum_v \log |\alpha|_v v$  as in the previous lecture, it follows that  $\epsilon$  is in the kernel of  $\lambda$ , which is exactly the set  $\mu$  of roots of unity in  $A$ .  $\square$

**Definition.** A unit  $\epsilon$  of  $A$  is called a *Lehmer unit* if all but two of its conjugates lie on the unit circle in  $\mathbb{C}$ . More precisely, if  $\sigma_1, \dots, \sigma_n$  are the distinct embeddings of  $k$  in  $\mathbb{C}$  and  $|\cdot|$  is the standard absolute value on  $\mathbb{C}$ , then for some  $i \neq j$ ,  $|\sigma_i(\epsilon)|, |\sigma_j(\epsilon)| \neq 1$  and for  $l \neq i, j$ ,  $|\sigma_l(\epsilon)| = 1$ .

If  $\epsilon$  is a Lehmer unit, then the fact that  $1 = \prod_{v|\infty} |\epsilon|_v = \sigma_i(\epsilon)\sigma_j(\epsilon)$  implies that  $\sigma_j(\epsilon) = \sigma_i(\epsilon)^{-1} = \overline{\sigma_i(\epsilon)}$ . For example, if  $k$  is a real quadratic field, and  $\alpha$  is a unit in the interval  $(0, 1)$ , then for the nontrivial embedding  $\sigma$ ,  $\sigma(\alpha) = 1/\alpha$  is in the interval  $(1, \infty)$  and  $\alpha$  is a Lehmer unit. In fact, if  $\epsilon$  is a Lehmer unit and  $\sigma$  and  $\tau$  are the embeddings such that  $|\sigma(\epsilon)|, |\tau(\epsilon)| \neq 1$ , then  $\sigma(\epsilon)$  and  $\tau(\epsilon)$  must be real. If not, say  $\sigma(\epsilon)$  is not real, then  $\overline{\sigma(\epsilon)}$  is another conjugate of  $\epsilon$ . Since  $|\overline{\sigma(\epsilon)}| = |\sigma(\epsilon)| \neq 1$ , it follows that  $\overline{\sigma(\epsilon)} = \tau(\epsilon)$ . However, the fact that

$$|\tau(\epsilon)| = \frac{1}{|\sigma(\epsilon)|} = \frac{1}{|\overline{\sigma(\epsilon)}|} \neq 1$$

implies that  $|\tau(\epsilon)| \neq |\overline{\sigma(\epsilon)}|$ . It is natural to ask whether or not there are Lehmer units which are not roots of unity and whose real conjugates get arbitrarily close to 1. Lehmer conjectured that this could not occur.

**Example.** Let  $\ell$  be a prime number  $\ell \geq 3$ ,  $\zeta$  a primitive  $\ell$ th root of unity, and  $k = \mathbb{Q}(\zeta)$ . By Proposition 36, the ring of integers of  $k$  is  $A = \mathbb{Z}[\zeta]$ .  $k$  is Galois over  $\mathbb{Q}$  with Galois group  $G$  which is cyclic of order  $n = \ell - 1 = 2r_2$  since  $k$  has no real embeddings. Then  $r_1 = 0$  and  $r_2 = \frac{\ell-1}{2}$ , and by the Unit Theorem,  $A^\times$  has rank  $r_1 + r_2 - 1 = \frac{\ell-3}{2}$ . Since  $G$  is cyclic of even order, it has a unique subgroup of order 2 whose nontrivial element is given by complex conjugation. Under the Galois Correspondence, the fixed field  $k^+$  of this subgroup is the unique intermediate field of degree  $\frac{\ell-1}{2}$  over  $\mathbb{Q}$ . Let  $A^+$  denote the ring of algebraic integers in  $k^+$ . Clearly,  $\mathbb{Z}[\zeta + \zeta^{-1}] \subseteq A^+$ , and a discriminant computation shows equality. (One must verify directly that  $\text{disc}(A^+) = \ell^{\binom{\ell-3}{2}}$ .) Since  $k^+$  is the fixed field of complex conjugation,  $k^+$  is a real field. It follows from a little Galois theory that,  $r_1^+ = n^+ = \frac{\ell-1}{2}$  and  $r_2^+ = 0$ . We verify this in more generality below. Again by the Unit Theorem, the rank of  $(A^+)^\times$  is  $\frac{\ell-3}{2}$ . Since  $(A^+)^\times \subseteq A^\times$  and these finitely generated groups have the same rank, the index  $(A^\times : (A^+)^\times)$  is finite.

More generally, let  $k$  be a number field which is totally complex (i.e.,  $r_1 = 0$ ) which therefore has degree  $n = 2r_2$  over  $\mathbb{Q}$ . Furthermore, assume that  $k$  is a quadratic extension of a totally real field  $k^+$ . ( $k$  is called a *CM field* in this event.) Assuming that  $k \subset \mathbb{C}$ , we let  $\tau : k \rightarrow \mathbb{C}$  denote the embedding of  $k$  corresponding to complex conjugation. That is, if  $\sigma$  is a fixed

embedding of  $k$ , then  $\tau = \bar{\sigma}$ . We let  $k^+$  denote the fixed field of  $\tau$ , or equivalently,  $k^+ = k \cap \mathbb{R}$ . Note that if  $\sigma$  is any embedding of  $k$  in  $\mathbb{C}$ , then  $\bar{\sigma} = \sigma \circ \tau$  is the embedding of  $k$  conjugate to  $\sigma$  and  $\{\sigma, \bar{\sigma}\}$  are the same real embedding of  $k^+$ . That is, there is a 1–1 correspondence between real embeddings of  $k^+$  and conjugate pairs of embeddings of  $k$ . Furthermore,  $(A^+)^{\times}$  has finite index in  $A^{\times}$ , as both groups have rank  $r_2 - 1$ .

Let  $u$  be a unit in  $A$ , and let  $\epsilon = u/\tau(u)$ . Then for any infinite place  $v$  of  $k$ ,

$$|\epsilon|_v = \frac{|\sigma(u)|}{|\overline{\sigma(u)}|} = 1$$

so that  $\epsilon$  is a root of unity by Corollary 46. It follows that  $\tau(u) = \epsilon u$  for a root of unity  $\epsilon$ . If  $\beta$  is another root of unity in  $k$ , then  $\tau(\beta u) = \beta^{-1} \epsilon u = \frac{\epsilon}{\beta^2} (\beta u)$ . Of course,  $\frac{\epsilon}{\beta^2}$  is another root of unity. It follows that if we let  $\epsilon = \beta^2$  and  $u' = \beta u$ , then  $u'$  is in the fixed field of  $\tau$ , that is,  $u' \in k^+$ . Since  $u'$  is an algebraic integer,  $u' \in A^+$ . Also,  $u'$  is a unit in  $A^+$ , as is shown by Lemma 40 and the correspondence between real embeddings of  $k^+$  and conjugate pairs of embeddings of  $k$ .

Let  $\mu$  denote the set of roots of unity in  $k$ , and consider the map  $\phi : A^{\times} \rightarrow \mu/\mu^2$  given by  $u \mapsto u/\tau(u)$ . The previous paragraph shows  $\phi$  is well-defined and has kernel exactly  $(A^+)^{\times} \cdot \mu$ . Since  $\mu$  is finite cyclic, it follows that  $\mu/\mu^2 \cong \mathbb{Z}/2\mathbb{Z}$ . Thus, the index of  $(A^+)^{\times} \cdot \mu$  in  $A^{\times}$  is 1 or 2, depending on whether  $\phi$  is trivial or not. For example, if  $k = \mathbb{Q}(\zeta)$  is the cyclotomic field from above, then  $(A^+)^{\times} \cdot \mu = A^{\times}$ . Since  $(A^+)^{\times} \cap \mu = \{\pm 1\}$ , this is not a direct product, but if  $\mu'$  denotes the set of  $\ell$ th roots of unity, then  $(A^+)^{\times} \times \mu' = A^{\times}$ , as  $\ell$  is odd by assumption.

Recall the notation from Lectures 6 and 7. If  $\zeta$  is a primitive  $\ell$ th root of unity, let  $\pi = \zeta - 1$ . For integers  $a$  such that  $2a \not\equiv 0 \pmod{\ell}$ , let  $\alpha(a) = \zeta^a - \zeta^{-a} = (\zeta^{2a} - 1)(\zeta^{-a})$ . We claim that  $\alpha(a)$  has norm  $\ell$ . From our earlier computations,  $\mathbb{N}(\zeta) = 1$  and  $\mathbb{N}(\pi) = \ell$ . Since  $\zeta^{2a} - 1$  is a conjugate of  $\pi$  and  $\zeta^{-a}$  is a conjugate of  $\zeta$  we see that  $\mathbb{N}(\alpha(a)) = \mathbb{N}(\pi)\mathbb{N}(\zeta) = \ell$ . Also, it is straightforward to check that  $\tau(\alpha(a)) = -\alpha(a)$ . Let

$$u_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}} = \frac{\alpha(a)}{\alpha(1)}$$

(We call  $u_a$  a *circular unit* because if  $\zeta = e^{2\pi i/\ell}$  then

$$u_a = \frac{e^{2\pi ai/\ell} - e^{-2\pi ai/\ell}}{e^{2\pi i/\ell} - e^{-2\pi i/\ell}} = \frac{\sin(2\pi a/\ell)}{\sin(2\pi/\ell)}$$

which is an expression in terms of the circular function  $\sin$ .) We claim that  $u_a$  is a unit in  $A^+$ . To see this, it suffices to show that  $u_a$  is a unit in  $A$  which is fixed by  $\tau$ , since then  $u_a$  is in  $A^+$  and  $\tau(u_a^{-1}) = \tau(u_a)^{-1} = u_a^{-1}$  so that  $u_a^{-1} \in A^+$ . Since  $\mathbb{N}(\alpha(a)) = \ell$ , we see that  $\mathbb{N}(u_a) = \ell/\ell = 1$ . Furthermore,  $u_a$  can be expressed as a polynomial in the algebraic integers  $\zeta, \zeta^{-1}$  so that  $u_a$  is an algebraic integer. Thus,  $u_a$  is a unit in  $A$ . Finally, since  $\tau(\alpha(a)) = -\alpha(a)$ , it follows that  $\tau(u_a) = u_a$ . To get distinct  $\alpha(a)$  up to sign, we can allow  $a$  to run from 1 to  $\frac{\ell-1}{2}$ . The choice  $a = 1$  gives  $u_a = 1$ , so we have  $\frac{\ell-3}{2}$  reasonable choices for  $a$ . In fact, we have the following theorem.

**Theorem 47.** (*Kummer*) *Let  $U$  be the subgroup of  $(A^+)^{\times}$  generated by the  $u_a$ . Then  $U$  is a free abelian group of rank  $\frac{\ell-3}{2}$  and the index of  $U$  in  $(A^+)^{\times}$  is finite and divisible by 2. Furthermore, if  $h^+$  is the class number of  $A^+$ , then the index is exactly  $2h^+$ .*

The proof of this theorem involves the theory of  $L$ -functions, so we omit it here (cf. Borevich and Shafarevich *Number Theory*, Chapter 5). However, we check an example.

**Example.** Let  $\ell = 5$ . Then  $u_2 = \frac{\zeta^2 - \zeta^{-2}}{\zeta - \zeta^{-1}} = \zeta + \zeta^{-1}$ . Since  $k$  has degree 4 over  $\mathbb{Q}$ , the field  $k^+$  is real quadratic, so  $k^+ = \mathbb{Q}(\sqrt{D})$  for some square free positive integer  $D$ . The nontrivial element of  $\text{Gal}(k^+/\mathbb{Q}) = \text{Gal}(k/\mathbb{Q})/\text{Gal}(k/k^+)$  is given by sending  $\zeta \mapsto \zeta^2$ . Thus,

$$\text{Tr}(u_2) = (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$$

by examining the minimal polynomial of  $\zeta$ , and

$$\mathbb{N}(u_2) = (\zeta + \zeta^{-1})(\zeta^2 + \zeta^{-2}) = \zeta^3 + \zeta^{-1} + \zeta + \zeta^{-3} = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$$

so that the minimal polynomial of  $u_2$  is  $x^2 + x - 1$ . The quadratic formula tells us that  $u = \frac{-1 \pm \sqrt{5}}{2}$  and by fixing an embedding, we may assume that  $u = \frac{-1 + \sqrt{5}}{2}$ . It follows that  $k^+ = \mathbb{Q}(\sqrt{5})$ , and a computation from Lecture 5 shows that  $h^+ = 1$ .

Next, we will discuss the tools developed by Chevalley, Artin, and Weil: completions of fields, the Adèles and the Idèles. These tools will give us a succinct reinterpretation of the finiteness of the ideal class group and the Unit Theorem. In much of the following discussion, only sketches of proofs will be given. The interested reader is invited to supply the missing details.

Recall that we construct infinite valuations on a number field from its embeddings in  $\mathbb{C}$ . These valuations satisfy the Archimedean property: for all  $x, y \in k^\times$  there exists an integer  $n$  such that  $|nx|_v > |y|_v$ . This follows from the fact that the absolute values on  $\mathbb{C}$  and  $\mathbb{R}$  are Archimedean. The finite valuations are those induced by nonzero prime ideals  $P$  in  $A$  by the formula  $|x|_P = \mathbb{N}(P)^{-\text{ord}_P(x)}$ . It follows that  $|\alpha + \beta|_P \leq \max\{|\alpha|_P, |\beta|_P\} \leq |\alpha|_P + |\beta|_P$ . Another way to express the first inequality is to say that all triangles are isosceles, since equality holds in the first inequality exactly when  $|\alpha|_P \neq |\beta|_P$ . However, the finite valuations do not satisfy the Archimedean property: since  $\mathbb{Z} \subseteq A$ , any integer  $n$  has  $|n|_P \leq 1$  so that  $|nx|_P = |n|_P|x|_P \leq |x|_P$ .

We recall the construction of the real numbers from the rationals. With the standard absolute value on  $\mathbb{Q}$

$$|x| = \begin{cases} x & \text{if } x > 0 \\ -x & \text{if } x < 0 \end{cases}$$

we say that a sequence  $\{a_n\}$  is *Cauchy* if, for every  $\epsilon > 0$  there exists  $N$  such that  $n, m \geq N \Rightarrow |a_m - a_n| < \epsilon$ . The problem with  $\mathbb{Q}$  is that there exist (lots of) Cauchy sequences in  $\mathbb{Q}$  which do not converge to elements of  $\mathbb{Q}$ . Basically,  $\mathbb{R}$  is constructed by adjoining all the limits of Cauchy sequences in  $\mathbb{Q}$  to  $\mathbb{Q}$ . We will be more specific below.

**Definition.** A *valued field* is a field  $k$  with valuation  $|| : k^\times \rightarrow \mathbb{R}_+^\times$ . A valued field  $k$  is *complete* if every Cauchy sequence in  $k$  converges to an element of  $k$ . A *completion* of a valued field  $k$  is an extension field  $K$  satisfying the following properties: (1)  $K$  is a valued field which is complete and whose valuation extends the valuation on  $k$ ; and (2)  $K$  contains  $k$  as a dense subfield. We require property (2) for uniqueness purposes: without it,  $\mathbb{C}$  would be a completion of  $\mathbb{Q}$ .

**Theorem 48.** For a valued field  $k$  with valuation  $|\cdot|_v$ , a completion  $k_v$  exists and is unique up to unique continuous isomorphism. More precisely, if  $k_v$  and  $k'_v$  are completions of  $k$ , then there exists a unique continuous isomorphism  $k_v \rightarrow k'_v$  making the following diagram commute.

$$\begin{array}{ccc} k_v & \xrightarrow{\quad} & k'_v \\ & \searrow & \nearrow \\ & k & \end{array}$$

*Sketch of proof.* Let  $R$  be the ring of all Cauchy sequences  $\{a_n\}$  with  $a_n \in k$ . Let  $\mathfrak{m}$  denote the (maximal) ideal of  $R$  consisting of all null sequences, that is, sequences  $\{a_n\}$  such that  $\lim_{n \rightarrow \infty} |a_n|_v = 0$ . We define  $k_v$  to be the quotient  $k_v = R/\mathfrak{m}$ , which is the field of limits of Cauchy sequences in  $k$ . We claim that this is a completion of  $k$ . We first extend the valuation from  $k$  to  $k_v$  in the natural way

$$|\cdot|_v : k_v^\times \rightarrow \mathbb{R}_+^\times \quad \text{as} \quad |\{a_n\}|_v = \lim_{n \rightarrow \infty} |a_n|_v \in \mathbb{R}$$

We embed  $k$  in  $k_v$  as the constant sequences

$$k \rightarrow k_v \quad \text{as} \quad a \mapsto \{a, a, a, \dots\}$$

since the constant sequences are trivially Cauchy.

Under this embedding,  $k$  is dense in  $k_v$ . Fix any  $\alpha = \{a_n\} \in k_v$ , and define a Cauchy sequence  $\alpha_1, \alpha_2, \dots$  of elements in the image of  $k$  in  $k_v$  as  $\alpha_i = \{a_i, a_i, \dots\}$ . Then  $\alpha = \lim_{n \rightarrow \infty} \alpha_i$ . Finally,  $k_v$  is complete. Fix a Cauchy sequence in  $k_v$ ,  $\alpha^i = \{\alpha_n^i\} = \{\alpha_1^i, \alpha_2^i, \dots\}$ . We want to show that this sequence converges to an element of  $k_v$ . Let  $\beta$  denote the “diagonal” sequence  $\beta = \{\alpha_1^1, \alpha_2^2, \dots\}$ . It is straightforward to show that  $\beta = \lim_{n \rightarrow \infty} \alpha^n$ . The uniqueness result is left as an easy exercise.  $\square$

**Example.** Let  $k = \mathbb{Q}$  and  $P = p\mathbb{Z}$  for a prime number  $p$ . The completion of  $\mathbb{Q}$  with respect to the valuation  $|\cdot|_P$  is denoted  $\mathbb{Q}_p$  and called the *p-adic numbers*. It will follow from more general work that the ring of integers in  $\mathbb{Q}_p$  is exactly  $\mathbb{Z}_p = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})$ .

More generally, if  $k$  is a number field and  $P$  is a nonzero prime ideal in  $A$  of characteristic  $p$ , then the completion of  $k$  with respect to the valuation  $|\cdot|_P$  is denoted  $k_P$ . We shall see that  $k_P$  is a finite extension of  $\mathbb{Q}_p$  of degree  $e_P f_P$ , where  $e_P$  is the ramification index of  $P$  and  $f_P$  is the residue degree.

## Lecture 10

We continue with the notation from the previous lecture. Given a nonzero prime ideal  $P$  in  $A$ , let  $q = \mathbb{N}(P)$ . Then the valuation  $|\cdot|_P$  on  $k$  takes its values in  $q^{\mathbb{Z}}$ . Since the valuation is non-Archimedean, if the sequence  $\{a_n\}$  is Cauchy with respect to  $|\cdot|_P$ , then the sequence  $\{|a_n|_P\}$  in  $q^{\mathbb{Z}} \subset \mathbb{Q}$  must stabilize. It follows that the valuation on  $k_P$  also takes its values in  $q^{\mathbb{Z}}$ . It also follows that the extended valuation is non-Archimedean. Define

$$A_P = \{\alpha \in k_P : |\alpha|_P \leq 1\}$$

and

$$P_P = \{\alpha \in k_P : |\alpha|_P < 1\} = \{\alpha \in k_P : |\alpha|_P \leq \frac{1}{q}\}$$

The fact that the valuation is non-Archimedean implies that  $A_P$  is a subring of  $k_P$  and that  $P_P$  is an ideal in  $A_P$ . Furthermore, restricting the embedding  $k \hookrightarrow k_P$  to  $A$  and  $P$  induces a commuting diagram

$$\begin{array}{ccccc} P_P & \subset & A_P & \subset & k_P \\ \uparrow & & \uparrow & & \uparrow \\ P & \subset & A & \subset & k \end{array}$$

**Proposition 49.**  $A_P$  is a discrete valuation ring with maximal ideal  $P_P$ .

*Proof.* Since  $P \neq 0$ , we know that  $P^2 \subsetneq P$ . Fix an element  $\pi \in P \setminus P^2$ , that is, such that  $|\pi|_P = \frac{1}{q}$ . The fact that  $P_P = \pi A_P$  will follow immediately from the following theorem.

**Theorem 50.** Let  $I$  be any nonzero ideal of  $A_P$  and suppose that

$$\max\{|\alpha|_P : 0 \neq \alpha \in I\} = q^{-m}$$

for some  $m \geq 0$ . Then  $I = \beta A_P$  for some  $\beta \in I$  such that  $|\beta|_P = q^{-m}$ .

*Proof.* First, we note that  $\max\{|\alpha|_P : 0 \neq \alpha \in I\}$  is always of the form  $q^{-m}$ . This follows from the fact that  $\{\text{ord}_P(\alpha) : 0 \neq \alpha \in I\}$  is a nonempty set of natural numbers. Furthermore, there is an element  $\beta$  of  $I$  with  $|\beta|_P = q^{-m}$  and we fix such an element. Clearly,  $I \supseteq \beta A_P$ . Conversely, if  $\alpha \in I$ , then  $|\alpha/\beta|_P \leq 1$  so that  $\gamma = \alpha/\beta \in A_P$  which implies that  $\alpha = \gamma\beta \in \beta A_P$ .  $\square$

From the proof of the theorem, we see that  $P_P = \pi A_P$ . Furthermore, if  $P_P$  were not maximal, then there would be some proper ideal  $I$  of  $A_P$  such that  $P_P \subsetneq I$ . By the theorem,  $I = \beta A_P$  for some  $\beta \in I$ . If  $\beta$  were in  $P_P$ , then  $I = P_P$ , so that  $\beta \notin P_P$ . It follows that  $1 \geq |\beta|_P \geq 1$  so that  $|\beta|_P = 1$ . This implies that  $|\beta^{-1}|_P = |\beta|_P^{-1} = 1$  so that  $\beta^{-1} \in A_P$  which implies that  $I = A_P$ . It follows exactly from this logic that the units of  $A_P$  are exactly those elements  $\alpha$  of  $k_P$  such that  $|\alpha|_P = 1$ .

To finish the proof of the proposition, it suffices to show that every nonzero ideal  $I$  of  $A_P$  is of the form  $\pi^m A_P$ . Let  $m$  and  $\beta$  be as in the theorem. Then  $|\beta/\pi^m|_P = 1$  so that  $\beta/\pi^m$  is a unit in  $A_P$  and  $I = \beta A_P = \pi^m A_P$ .  $\square$

Restricting the embedding  $k \hookrightarrow k_P$  to the ideals  $P^n$  induces another commuting diagram

$$\begin{array}{ccccccccc} \cdots & \pi^n A_P & \subset & \cdots & \subset & \pi^2 A_P & \subset & \pi A_P & \subset & A_P & \subset & k_P \\ & \uparrow & & & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \cdots & P^n & \subset & \cdots & \subset & P^2 & \subset & P & \subseteq & A & \subset & k \end{array}$$

**Proposition 51.** With notation as above.

1. The ring  $A$  is dense in  $A_P$ .

2. The inclusion  $A \hookrightarrow A_P$  induces an isomorphism  $A/P^n \cong A_P/\pi^n A_P$  for  $n = 1, 2, \dots$
3.  $A_P = \varprojlim_n (A/P^n)$ .

*Proof.* 1. For each  $x \in A_P$ , the fact that  $k$  is dense in  $k_P$  implies that for every  $\epsilon > 0$  there are  $\alpha, \beta \in A$  such that  $|\alpha/\beta - x|_P < \epsilon$ . Assuming that  $\epsilon \leq 1$ , the fact that  $|x|_P \leq 1$  implies that  $|\alpha/\beta|_P < 1$  since otherwise

$$\epsilon > |\alpha/\beta - x|_P = \max\{|\alpha/\beta|_P, |x|_P\} = |\alpha/\beta|_P \geq 1$$

Thus,  $\text{ord}_P(\alpha) \geq \text{ord}_P(\beta)$  so that  $\alpha \in P^{\text{ord}_P(\beta)}$ . It suffices to find an element  $\gamma \in A$  such that  $|\gamma - \alpha/\beta|_P < \epsilon$ , since then

$$|\gamma - x|_P \leq |\gamma - \alpha/\beta|_P + |\alpha/\beta - x|_P < 2\epsilon$$

It is equivalent to find  $\gamma \in A$  such that  $|\alpha - \gamma\beta|_P < \epsilon|\beta|_P$ . Furthermore, it suffices to show that  $\alpha \in \beta A + P^n$  for  $n \gg 0$ , as this implies that for each such  $n$  there exists  $\gamma_n \in A$  such that  $\alpha - \gamma_n\beta \in P^n$  (so that  $\text{ord}_P(\alpha - \gamma_n\beta) \geq n$ ) and if we choose  $n$  such that  $q^{-n} < \epsilon|\beta|_P$  then

$$|\alpha - \gamma_n\beta|_P = q^{-\text{ord}_P(\alpha - \gamma_n\beta)} \leq q^{-n} < \epsilon|\beta|_P$$

as desired. Claim: for  $n \geq \text{ord}_P(\beta)$ ,  $\beta A + P^n = P^{\text{ord}_P(\beta)}$ . Once the claim is proved, we are done, since we have already shown that  $\alpha \in P^{\text{ord}_P(\beta)}$ . Since  $P$  is maximal, the only ideal containing  $\beta A + P^n$  is  $P$ . Thus, the prime decomposition of  $\beta A + P^n$  is of the form  $P^m$ . Since  $\beta \in \beta A + P^n = P^m$ , we see that  $m \leq \text{ord}_P(\beta)$ . And the fact that  $P^m = \beta A + P^n \subseteq P^{\text{ord}_P(\beta)}$  implies that  $m \geq \text{ord}_P(\beta)$ .

2. The ideal  $\pi^n A_P$  is both open and closed in  $A_P$ , as

$$\pi^n A_P = \{\alpha \in A_P : |\alpha|_P \leq \frac{1}{q^n}\} = \{\alpha \in A_P : |\alpha|_P < \frac{1}{q^{n-1}}\}$$

Since  $A$  is dense in  $A_P$  and the coset  $\alpha + \pi^n A_P$  is open for each  $\alpha \in A_P$ , it follows that  $A \cap (\alpha + \pi^n A_P) \neq \emptyset$ . This implies that the map  $A \rightarrow A_P/\pi^n A_P$  is surjective for every  $n$ . Furthermore, the kernel is exactly  $\pi^n A_P \cap A$ . If we can show that this is exactly  $P^n$ , then we are done. This is clear, though, since  $\pi^n A_P \cap A$  is exactly the collection of elements  $\alpha$  of  $A$  with  $|\alpha|_P \leq q^{-n}$ , and this is exactly  $P^n$ .

3. By the completeness of  $A_P$  we see that  $A_P = \varprojlim_n (A_P/\pi^n A_P) = \varprojlim_n (A/P^n)$ . □

It follows from 3. that  $A_P$  is a compact topological ring, as it is the projective limit of finite (and therefore compact) topological rings. (We say that  $A_P$  is *profinite*.) Furthermore,  $k_P$  is locally compact as for every  $\alpha \in k_P$ , the translate  $\alpha + A_P$  is a compact neighborhood. The advantage of working in  $k_P$  instead of  $\mathbb{R}$  or  $\mathbb{C}$  is that, in  $k_P$ ,  $A$  is contained in the compact subring  $A_P$ . The images of  $A$  in  $\mathbb{R}$  and  $\mathbb{C}$  have no hope of being compact, as they are unbounded.

Recall that the Tychonoff Theorem implies that, with the product topology, the topological ring  $\prod_{P \neq 0} A_P$  is compact, where the product is taken over all nonzero prime ideals  $P$  of  $A$ . The diagonal embedding  $A \rightarrow \prod_P A_P$  given by  $a \mapsto (a, a, \dots)$  is a topological ring homomorphism.

**Proposition 52.** *The image of  $A$  under the diagonal embedding  $A \rightarrow \prod_P A_P$  is a dense subring.*

*Proof.* By the definition of the product topology, to approach an element  $x \in \prod_P A_P$ , we must find  $\alpha \in A$  which is arbitrarily close to  $x$  in any number of coordinates, indexed by a finite set of prime ideals. That is, if  $P_1, \dots, P_m$  are prime ideals and  $m_i > 0$  for  $i = 1, \dots, m$ , then we need to find an element  $\alpha \in A$  such that  $|\alpha - \alpha_i|_{P_i} < q_i^{-m_i}$  for  $i = 1, \dots, m$ . This is equivalent to finding an element  $\alpha$  such that  $\alpha \equiv \alpha_i$  in  $A_{P_i}/(P_i)^{m_i} = A/P_i^{m_i}$  for each  $i$ . The Chinese Remainder Theorem tells us that the homomorphism  $A \rightarrow \prod_i A/P_i^{m_i}$  is surjective, since  $i \neq j \Rightarrow P_i + P_j = A$ . The result now follows.  $\square$

We want a ring  $R$  which has the same properties with respect to  $k$ . That is,  $R$  should be locally compact and  $k$  should embed in  $R$  naturally. With the proposition in mind, our first candidate for  $R$  is  $\prod_v k_v$  where the product is taken over all (finite and infinite) places. However, since the  $k_v$  are only locally compact (and not compact) and the product is infinite, this ring is no longer locally compact. The next reasonable candidate is  $\prod_v k_v$ , which is locally compact. However, the diagonal map  $k \rightarrow \prod_v k_v$  is not well-defined. Therefore, the ring we want should be somewhere in between the coproduct and the product. This leads us to the Adèles  $\mathbb{A}$  which is the locally compact subring of  $\prod_v k_v$  consisting of those  $(a_v)$  such that  $a_P \in A_P \subset k_P$  for almost all  $P$ . The diagonal embedding  $k \rightarrow \prod_v k_v$  lands in  $\mathbb{A}$  since, for  $\alpha \in k$ ,  $\text{ord}_P(\alpha) = 0$  for all but finitely many  $P$ .

We describe the construction in a slightly more general context. Assume that  $V$  is some set indexing a collection of locally compact (abelian) groups  $\{G_v\}$ . How do we construct a locally compact subgroup of  $\prod_v G_v$ ? Under an additional hypothesis we will do this via a “restricted” direct product  $\prod_v G_v$ . Assume that, for all but finitely many  $v \in V$ , there is a distinguished compact, open subgroup  $H_v$  of  $G_v$ . Let  $V_\infty$  denote the finite collection of indices for which there is no  $H_v$ . The restricted direct product is then the subgroup  $G = \prod_v G_v$  of  $\prod_v G_v$  consisting of those  $(g_v)$  such that  $g_v \in H_v$  for almost all  $v \in V \setminus V_\infty$ . If  $S$  is a finite subset of  $V$  containing  $V_\infty$ , then let

$$G_S = \left( \prod_{v \in S} G_v \right) \times \left( \prod_{v \notin S} H_v \right)$$

Since each  $G_v$  is locally compact and  $S$  is finite,  $\prod_{v \in S} G_v$  is locally compact as well. And since each  $H_v$  is compact,  $\prod_{v \notin S} H_v$  is also compact. It follows immediately that  $G = \cup_S G_S$  where the union is taken over all such finite sets  $S$ . We also notice that if  $S \subseteq T$ , then  $G_S \subseteq G_T$  is an open subgroup. Thus, the collection of  $G_S$  give an open system of neighborhoods for a topology on  $G$  which is locally compact. (Note that this is not the topology induced by the product topology on  $\prod_v G_v$ .)

If  $V$  now denotes the collection of (finite and infinite) valuations on  $k$ , we may take  $G_v = k_v$  and for nonzero prime ideals  $P$  of  $A$ ,  $H_P = A_P$ . In the previous notation,  $V_\infty$  is the collection of infinite valuations on  $k$ . For any finite subset  $S$  of  $V$  containing  $V_\infty$ , we then have

$$\mathbb{A}_S = \left( \prod_{v \in S} k_v \right) \times \left( \prod_{P \notin S} A_P \right)$$

The benefit of the generality of the previous paragraph is that we can apply the same construction to the units of  $\mathbb{A}$ , taking  $G_v = k_v^\times$  and  $H_P = A_P^\times$ . The resulting restricted direct product  $J$  is called the *idèles*. As abelian groups,  $J = \mathbb{A}^\times$ .

To convey somewhat the structure of  $k_P^\times$ , consider the short exact sequence of abelian groups

$$1 \rightarrow A_P^\times \rightarrow k_P^\times \xrightarrow{\text{ord}_P} \mathbb{Z} \rightarrow 1$$

which necessarily splits. We see that a filtration on  $A_P^\times$  will then induce a filtration on  $k_P^\times$ . Recall that a filtration of the ring  $A_P$  was given by powers of the maximal ideal  $P_P$

$$\cdots \subset P_P^3 \subset P_P^2 \subset P_P \subset A_P$$

and since each  $P_P^i = \pi^i$ , it follows that each quotient in the filtration is a one dimensional vector space over the finite field  $A_P/P_P \cong A/P$ . The filtration of  $A_P^\times$  is given by translates of powers of the maximal ideal

$$\cdots \subset 1 + P_P^3 \subset 1 + P_P^2 \subset 1 + P_P \subset A_P^\times$$

The first quotient is

$$A_P^\times / (1 + P_P) \cong (A/P)^\times$$

and for  $i \geq 1$ ,

$$(1 + P_P^i) / (1 + P_P^{i+1}) \cong A/P$$

For more details, the interested reader should consult Serre *Local Fields*, Chapter IV, SS2..

As we noted above, the diagonal embedding  $k \rightarrow \prod_v k_v$  is a continuous homomorphism of rings which lands in  $\mathbb{A}$ . The restriction to  $k^\times$  is a continuous homomorphism of abelian groups which lands in  $\mathbb{A}^\times$ . In addition, we have the following.

**Proposition 53.** *With notation as above,*

1.  $k$  is a discrete subring of  $\mathbb{A}$  and the quotient  $\mathbb{A}/k$  is compact.
2.  $k^\times$  is a discrete subgroup of  $J$ , and the quotient  $J/k^\times$  is almost compact.

**Definition.** A space  $X$  is *almost compact* if it is of the form  $C \times \mathbb{R}$  where  $C$  is compact. In the situation of the proposition, we can be more specific. There is a canonical surjective homomorphism  $\|\cdot\| : J \rightarrow \mathbb{R}_+^\times$  given by  $(a_v) \mapsto \prod_v |a_v|_v$ . This is well-defined since the product is always finite. It is a multiplicative homomorphism, as each  $|\cdot|_v$  is multiplicative. It is surjective, as  $k$  has at least one infinite place  $v$ . The completion  $k_v$  is isomorphic to  $\mathbb{R}$  or  $\mathbb{C}$  as a valued field, and therefore  $|\cdot|_v : k_v^\times \rightarrow \mathbb{R}_+^\times$  is surjective. To see that  $\|\cdot\|$  is surjective, we apply it to an element of the form  $(1, \dots, a_v, 1, \dots)$  where the non-identity entry is in the place indexed by the distinguished  $v$ . Furthermore, the kernel, which we shall denote by  $J_1$ , contains the image of  $k^\times$ , by the product formula (Theorem 42). Since the quotient  $J/J_1 \cong \mathbb{R}_+^\times$  is isomorphic to the additive group of real numbers, part 2 of Proposition 53 is equivalent to the fact that  $J_1/k^\times$  is compact.

*Sketch of proof.* If we write

$$\prod_{\text{all } v} k_v = \prod_{v|\infty} k_v \times \prod_{v \nmid \infty} k_v$$

then  $\mathbb{A} \subset \prod_{\text{all } v} k_v$  has two distinguished subsets, namely

$$\prod_{v|\infty} k_v \times 1 \quad \text{and} \quad 1 \times \prod_{v \nmid \infty} A_v$$

As we noted above,  $\prod_{v|\infty} k_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ , which contains  $A$  as a discrete, co-compact subset. Let  $D_\infty$  denote the fundamental domain for  $A$  acting on  $\prod_{v|\infty} k_v$ , which has compact closure, by co-compactness. Let  $U_\infty \subset \mathbb{R}^n$  be an open subset containing 0 such that  $A \cap U_\infty = (0)$ , which exists by discreteness. Consider the subset

$$D = D_\infty \times \prod_{v \nmid \infty} A_v \subset \mathbb{A}$$

which has compact closure.

1.  $D$  is a fundamental domain for  $k$  acting on  $\mathbb{A}$ , i.e.,  $\mathbb{A}$  is the disjoint union of translates  $\mathbb{A} = \cup_{\alpha \in k} (\alpha + D)$ , so the quotient  $\mathbb{A}/k$  is compact. Let

$$U = U_\infty \times \prod_{v \nmid \infty} A_v \subset \mathbb{A}$$

which is an open subset. Then  $U \cap k = (0)$ , as

$$k \cap \left( 1 \times \prod_{v \nmid \infty} A_v \right) = A$$

Thus,  $k$  is discrete in  $\mathbb{A}$ .

2. If we now let

$$U = \prod_{v|\infty} k_v^\times \times \prod_{v \nmid \infty} A_v^\times$$

then  $U$  is an open subgroup of  $J$  and  $U \cap k^\times = A^\times$ . Using a bounded region in  $\prod_{v|\infty} k_v^\times$ , we can find a smaller open subset  $U_0$  such that  $U_0 \cap k^\times = (0)$ . Thus,  $k^\times$  is discrete in  $J$ . Since  $U \cap k^\times = A^\times$ , it follows that  $k^\times \cdot U/U = k^\times/A^\times$ . If we let  $\mathbf{I}$  denote the group of all fractional ideals of  $A$ , let  $\mathbf{P}$  denote the subgroup of principal fractional ideals and let  $C$  denote the ideal class group, then we have the following commuting diagram

$$\begin{array}{ccccccccc}
& & & & 1 & & 1 & & \\
& & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U & \longrightarrow & k^\times \cdot U & \longrightarrow & k^\times / A^\times & \equiv & \mathbf{P} \longrightarrow 1 \\
& & \parallel & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U & \longrightarrow & J & \longrightarrow & \prod_P \mathbb{Z} & \equiv & \mathbf{I} \longrightarrow 1 \\
& & & & \downarrow & & \downarrow & & \\
& & & & J/(k^\times \cdot U) & & C & & \\
& & & & \downarrow & & \downarrow & & \\
& & & & 1 & & 1 & & 
\end{array}$$

in which the top two rows and the right-hand two columns are exact. It follows from the snake lemma that  $J/(k^\times \cdot U) \cong C$ , which is finite. The fact that  $J/(k^\times \cdot U)$  is finite and the following short exact sequence

$$1 \rightarrow U/A^\times \rightarrow J/k^\times \rightarrow J/(k^\times \cdot U) \rightarrow 1$$

show that the index of  $U/A^\times$  in  $J/k^\times$  is finite. Thus, to prove that  $J/k^\times$  is almost compact, it suffices to prove that  $U/A^\times$  is almost compact. We have an inclusion

$$A^\times \hookrightarrow U = \prod_{v|\infty} k_v^\times \times \prod_{v \nmid \infty} A_v^\times$$

and a short exact sequence

$$1 \rightarrow \underbrace{1 \times \prod_{v \nmid \infty} A_v^\times}_{\text{compact}} \rightarrow U/A^\times \rightarrow \left( \prod_{v|\infty} k_v^\times \right) / \text{Im}(A^\times) \rightarrow 1$$

so that we need only show that  $(\prod_{v|\infty} k_v^\times) / \text{Im}(A^\times)$  is almost compact. The short exact sequence

$$\begin{array}{ccccccc}
1 & \longrightarrow & \prod_{v \text{ real}} \{\pm 1\} \times \prod_{v \text{ cpx.}} S^1 & \longrightarrow & \prod_{v|\infty} k_v^\times & \xrightarrow{\lambda} & \bigoplus_{v|\infty} \mathbb{R}v \longrightarrow 1 \\
& & & & (\alpha_v) & \longmapsto & \sum_v \log |\alpha_v|_v v
\end{array}$$

induces a short exact sequence on quotients

$$1 \rightarrow \left( \prod_{v \text{ real}} \{\pm 1\} \times \prod_{v \text{ cpx.}} S^1 \right) / A_{\text{tor}}^\times \rightarrow \left( \prod_{v|\infty} k_v^\times \right) / \text{Im}(A^\times) \rightarrow \left( \bigoplus_{v|\infty} \mathbb{R}v \right) / \lambda(A^\times) \rightarrow 1$$

Since  $\prod \{\pm 1\} \times \prod S^1$  is compact, so is the quotient  $(\prod \{\pm 1\} \times \prod S^1) / A_{\text{tor}}^\times$ . The Unit Theorem implies that  $(\bigoplus_{v|\infty} \mathbb{R}v) / \lambda(A^\times)$  is almost compact. Thus,  $(\prod_{v|\infty} k_v^\times) / \text{Im}(A^\times)$  is almost compact and the proof is complete.  $\square$

Notice that we used the finiteness of the class group and the Unit Theorem at key steps of the proof. It can be shown that the conclusions of the proposition are actually equivalent to these two results. (For example, see A. Weil *Basic Number Theory*, Chapter V.)

## Lecture 11

Now we introduce the zeta function of a number field and study its properties. In particular, we discuss the classical Riemann zeta function.

For a number field  $k$  and integer  $n \geq 1$ , let  $a_n$  denote the number of integral ideals  $I$  of  $A$  with  $\mathbb{N}(I) = n$ . For example, if  $k = \mathbb{Q}$ , then  $A = \mathbb{Z}$  and  $a_n = 1$  for all  $n$  since the unique such ideal is  $n\mathbb{Z}$ . If  $k = \mathbb{Q}(\sqrt{D})$ , then to calculate  $a_n$ , we must know the factorization of primes  $p$  in  $A$ . For example, if  $pA = P_1P_2$  for distinct primes  $P_1$  and  $P_2$ , then the ideals of index  $p$  are exactly the primes of characteristic  $p$ , namely, the  $P_i$ . The other cases are similar, and we summarize.

$$a_p = \begin{cases} 2 & \text{if } pA = P_1P_2 \text{ is split} \\ 1 & \text{if } pA = P^2 \text{ is ramified} \\ 0 & \text{if } pA = P \text{ is inert} \end{cases}$$

We can apply the same methods to  $a_{p^2}$ .

$$a_{p^2} = \begin{cases} 3 & \text{if } pA = P_1P_2 \text{ is split: the ideals are } P_1^2, P_2^2, \text{ and } P_1P_2 = pA \\ 1 & \text{if } pA = P^2 \text{ is ramified: the ideal is } P^2 = pA \\ 1 & \text{if } pA = P \text{ is inert: the ideal is } P = pA \end{cases}$$

**Definition.** Using the above notation, we define the *zeta function* of  $k$  as the formal series

$$\zeta_k(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where  $s$  is a complex variable.

**Example.** If  $k = \mathbb{Q}$ , then we have the Riemann zeta function

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Most properties of general zeta functions will be proved for the Riemann zeta function first, and the general case will follow from the specific case.

First, we study general series of the form  $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$  with all  $a_i \in \mathbb{C}$ . (A series of this form is called a *Dirichlet series*.) Assume that there are fixed real numbers  $\sigma_0 \geq 0$  and  $K > 0$  such that  $|a_n| \leq Kn^{\sigma_0}$  for all  $n$ . (We say that  $a_n = O(n^{\sigma_0})$ .) Claim: Under these hypotheses, the Dirichlet series  $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$  converges absolutely and defines an analytic function of  $s$  in the open half-plane  $\operatorname{Re}(s) > \sigma_0 + 1$ . In particular, the derivative of  $f$  may be taken term by term, and the series may be treated as a finite sum in terms of products, on the set of convergence. We prove this by the comparison test. We have

$$|n^{-s}| = |e^{-s \log n}| = e^{\operatorname{Re}(-s \log n)} = e^{-\sigma \log n} = n^{-\sigma}$$

where  $\sigma = \operatorname{Re}(s)$ . By assumption then, we have the inequality

$$\left| \frac{a_n}{n^s} \right| \leq K \frac{1}{n^{(\sigma - \sigma_0)}} = K \frac{1}{n^{\rho}}$$

where  $\rho = \sigma - \sigma_0$ . Thus, we compare the series  $\sum_{n=1}^{\infty} \left| \frac{a_n}{n^s} \right|$  to the series  $\sum_{n=1}^{\infty} \left| \frac{1}{n^\rho} \right| = \sum_{n=1}^{\infty} \frac{1}{n^\rho}$ . The second series converges if  $\rho > 1$  (by the integral test) and diverges if  $\rho = 1$  (as this is the harmonic series). It follows that the original series converges absolutely for  $\sigma - \sigma_0 = \rho > 1$ , i.e., for  $\sigma > 1 + \sigma_0$ . Furthermore, for  $\epsilon > 0$  and  $c' \geq 1 + \epsilon$ , the second series converges uniformly for  $1 + \epsilon \leq \rho \leq c'$ . Thus,  $f(s)$  converges uniformly on compact subsets. Since each function in the sum is analytic, this proves the claim (cf. W. Rudin *Real and Complex Analysis*, Theorem 10.28). We rephrase the statement regarding products more precisely. Assume that  $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$  and  $g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$  are Dirichlet series which converge absolutely and define an analytic function of  $s$  in the open half-plane  $\operatorname{Re}(s) > \sigma_0 + 1$ . Then the product  $f(s)g(s)$  is another Dirichlet series

$$\left( \sum_{n=1}^{\infty} \frac{a_n}{n^s} \right) \left( \sum_{n=1}^{\infty} \frac{b_n}{n^s} \right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

which converges absolutely and defines an analytic function of  $s$  in the same open half-plane. The coefficients  $c_n$  are given by the formula

$$c_n = \sum_{\substack{de=n \\ d,e \geq 1}} a_d b_e$$

as expected.

We apply the claim to the Riemann zeta function. Since  $a_n = 1$  for all  $n$ , the constants  $\sigma_0 = 0$  and  $K = 1$  tell us that  $\zeta(s)$  is analytic on the open half-plane  $\operatorname{Re}(s) > 1$ . We shall prove later that the same convergence result holds for  $\zeta_k(s)$  where  $k$  is any number field. As noted,  $\zeta(s)$  does not converge at  $s = 1$ . We would like to know “how bad” the singularity is at  $s = 1$ .

**Lemma 54.** *The function  $f(s) = \zeta(s) - \frac{1}{s-1}$  has an analytic continuation to the open half-plane  $\operatorname{Re}(s) > 0$ . That is,  $\zeta(s)$  is meromorphic on  $\operatorname{Re}(s) > 0$  with unique pole at  $s = 1$  with residue  $\operatorname{Res}_{s=1} \zeta(s) = 1$ .*

*Proof.* For  $\operatorname{Re}(s) > 1$  we have

$$\int_1^{\infty} t^{-s} dt = \left. \frac{t^{1-s}}{1-s} \right|_1^{\infty} = \frac{1}{s-1}$$

Thus, for  $\operatorname{Re}(s) > 1$

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \left( \frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) \\ &= \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt \\ &= \sum_{n=1}^{\infty} \phi_n(s) \end{aligned}$$

where  $\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt$ . Note that each  $\phi_n(s)$  is defined for all  $s$ , and analytic on  $\mathbb{C}$ . As above, then, we need only show uniform convergence on compact subsets of  $\operatorname{Re}(s) > 0$ .

It is immediate that  $|\phi_n(s)| \leq \max_{n \leq t \leq n+1} |n^{-s} - t^{-s}|$ . For fixed  $n$ , let  $f_s(t) = n^{-s} - t^{-s}$ . The Taylor series for  $f_s(t)$  at  $t = n$  is given by

$$f_s(t) = n^{-s} - t^{-s} = f_s(n) + f'_s(n)(t - n) + R(t) = \frac{s}{n^{s+1}}(t - n) + R(t)$$

where  $R(t) = \frac{1}{2}f''_s(c)(t - n)^2$  for some  $c$  in the interval  $[n, n + 1]$ . The fact that  $|t - n| \leq 1$  on this interval implies that

$$|f_s(t)| \leq \frac{1}{n^{\sigma+1}}(|s| + \frac{1}{2}|s(s + 1)|)$$

where  $\sigma = \operatorname{Re}(s) > 0$ . As before, we have absolute convergence for  $\sigma > 0$  and uniform convergence on compact subsets of the half-plane, establishing the result.  $\square$

**Lemma 55.** *For  $\operatorname{Re}(s) > 1$  we have an infinite product expansion*

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

Essentially, this result is a restatement of the unicity of prime factorization. This product is nice because each factor is analytic and nonzero for  $\operatorname{Re}(s) > 0$ . This implies that  $\zeta(s)$  has no zeroes in the open half-plane  $\operatorname{Re}(s) > 1$ .

*Proof.* Let  $S$  be a finite set of prime numbers, and let  $N(S)$  denote the infinite set of integers  $n \geq 1$  whose prime factorization involves only the primes in  $S$ . The factor  $(1 - p^{-s})^{-1}$  has an expansion as a geometric series

$$\frac{1}{1 - p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \dots$$

so that formal multiplication yields

$$\prod_{p \in S} (1 - p^{-s})^{-1} = \sum_{n \in N(S)} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

for  $\operatorname{Re}(s) > 1$ . Notice that this inequality holds for all such finite sets  $S$ , and as  $S$  becomes sufficiently large,  $\sum_{n \in N(S)} \frac{1}{n^s} \rightarrow \sum_{n=1}^{\infty} \frac{1}{n^s}$ .  $\square$

**Corollary 56.** *As  $s \rightarrow 1$  inside  $\operatorname{Re}(s) > 1$*

$$\sum_p \frac{1}{p^s} \sim \log\left(\frac{1}{s - 1}\right)$$

where  $\sim$  means that the quotient tends to 1.

*Proof.*

$$\begin{aligned} \log(\zeta(s)) &= \log\left(\prod_p (1 - p^{-s})^{-1}\right) \\ &= \sum_p (-\log(1 - p^{-s})) \\ &= \sum_p \left(p^{-s} + \frac{p^{-2s}}{2} + \frac{p^{-3s}}{3} + \dots\right) \end{aligned}$$

using the Taylor expansion  $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots$

$$= \sum_p \frac{1}{p^s} + \sum_p \sum_{k \geq 2} \frac{p^{-ks}}{k}$$

The series  $\sum_p \sum_{k \geq 2} \frac{p^{-ks}}{k}$  is finite as  $s \rightarrow 1$  and is bounded by

$$\sum_p \sum_{k \geq 2} \frac{p^{-k}}{k} \leq \sum_p \frac{1}{p(p-1)} \leq \sum_{n \geq 2} \frac{1}{n(n-1)} < 1$$

By Lemma 54,

$$\log\left(\frac{1}{s}\right) \sim \log(\zeta(s)) \sim \sum_p \frac{1}{p^s}$$

as desired. □

**Corollary 57.** *The sum  $\sum_p \frac{1}{p}$  is infinite. In particular, there are an infinite number of prime numbers.*

*Proof.* Immediate. □

It has been shown that as  $x \rightarrow \infty$ , the function

$$\sum_{p \leq x} \frac{1}{p} \sim \log(\log(x))$$

Let  $\pi(x)$  denote the number of prime numbers  $p \leq x$ , or equivalently,  $\pi(x) = \sum_{p \leq x} 1$ .

**Theorem 58.** (*Prime Number Theorem*) *As  $x \rightarrow \infty$ ,*

$$\pi(x) \sim \frac{x}{\log(x)}$$

Riemann proved that the Prime Number Theorem is equivalent to the condition that  $\zeta(s)$  has no zeros with  $\operatorname{Re}(s) = 1$ ,  $s \neq 1$ . Hadamard then proved this statement. Furthermore, if we define  $\operatorname{li}x = \int_2^x \frac{dt}{\log t}$ , then it has been shown that

$$\pi(x) - \operatorname{li}x = O(xe^{-c(\log x)^{1/2}})$$

for a constant  $c$ , provided that  $\zeta(s)$  has no zeroes for  $\operatorname{Re}(s) \geq \rho$ . Along these lines, we have the Riemann Hypothesis, which is still unsolved.

**Conjecture 59.** (*Riemann*) *The only zeroes of  $\zeta(s)$  occur on the line  $\operatorname{Re}(s) = \frac{1}{2}$ .*

There is much computational evidence for this conjecture. Also, it has been shown that

$$\#\{\rho \leq t : \zeta\left(\frac{1}{2} + i\rho\right) = 0\} = \frac{t}{2\pi} \log \frac{t}{2\pi} - \frac{t}{2\pi} + O(\log t)$$

(c.f., Davenport, *Multiplicative Number Theory*, p. 59).

Since we have been studying the properties of  $\zeta(s) = \prod_p(1 - p^{-s})^{-1}$ , it seems reasonable for us to ask “What is  $\prod_p(1 - p^{-s})$ ?” We define the *Möbius function*  $\mu : \mathbb{Z}_+ \rightarrow \{0, \pm 1\}$  as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ (-1)^t & \text{if } n \text{ is square-free with } t \text{ distinct prime factors} \end{cases}$$

Then we have the formula  $\prod_p(1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ . The proof of this is an exercise in bookkeeping, and is left to the interested reader. From this, we can prove the following.

**Theorem 60.** (*Möbius Inversion*) *Assume that  $g : \mathbb{Z}_+ \rightarrow \mathbb{C}$  is a function such that for a fixed real number  $\sigma_0 \geq 0$ ,  $g(n) = O(n^{\sigma_0})$ . Define  $f : \mathbb{Z}_+ \rightarrow \mathbb{C}$  by the formula*

$$f(n) = \sum_{\substack{d|n \\ d \geq 1}} g(d)$$

*Then we can recover  $g$  from  $f$  by the formula*

$$g(n) = \sum_{\substack{n=de \\ d \geq 1}} f(d)\mu(e)$$

*Proof.* First, we observe that, given a sequence  $a_n$ , the formal series  $\sum_n \frac{a_n}{n^s}$  satisfies the following property

$$\sum_n \frac{f(n)}{n^s} = \sum_n \frac{g(n)}{n^s} \sum_n \frac{a_n}{n^s} \quad \text{iff} \quad f(n) = \sum_{n=de} g(d)a_e$$

This equivalence follows from the following expansion

$$\sum_n \frac{g(n)}{n^s} \sum_n \frac{a_n}{n^s} = \sum_d \frac{g(d)}{d^s} \sum_e \frac{a_e}{e^s} = \sum_{d,e} \frac{g(d)a_e}{(de)^s} = \sum_n \frac{\sum_{n=de} g(d)a_e}{n^s}$$

If we write  $f(n) = \sum_{n=de} g(d)a_e$ , then it follows that

$$\sum_n \frac{f(n)}{n^s} = \sum_n \frac{g(n)}{n^s} \sum_n \frac{1}{n^s} = \sum_n \frac{g(n)}{n^s} \zeta(s)$$

Multiplication by  $\zeta(s)^{-1} = \prod_p(1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$  yields

$$\sum_n \frac{g(n)}{n^s} = \sum_n \frac{f(n)}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

so that our first observation implies the desired formula. □

## Lecture 12

We now return to the general zeta function  $\zeta_k(s)$  for a number field  $k$ . As above, for  $n = 1, 2, \dots$ , let  $a_n$  denote the number of integral ideals  $I$  of  $A$  with norm  $\mathbb{N}(I) = n$ . If  $P$  is a prime ideal of  $A$  of characteristic  $p$ , then  $P$  occurs in the factorization of  $pA$ , so we write  $P|p$ . Formally, we have

$$\zeta_k(s) = \sum_{I \subset A} \frac{1}{\mathbb{N}(I)^s} = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_P \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \prod_p \left(\prod_{P|p} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}\right)$$

by the unicity of prime factorization of ideals. We want to show that  $\zeta_k(s)$  converges absolutely on the open half-plane  $\operatorname{Re}(s) > 1$  and describes an analytic function there. To accomplish this, we notice that the final expression may be written as

$$\lim_{x \rightarrow \infty} \prod_{p \leq x} \left(\prod_{P|p} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}\right)$$

We shall show that the finite product in the limit satisfies

$$\left| \prod_{p \leq x} \left(\prod_{P|p} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}\right) \right| \leq \zeta(s)^n$$

And therefore, the desired properties of  $\zeta_k(s)$  follow from the corresponding properties of  $\zeta(s)$ . It should be noted that the equalities for the infinite sums and products are purely formal. However, taking limits of finite sums and products shows that the series also converge, and they converge to the same function as the infinite products. The equality of the sum with the product will be crucial in proving certain properties. In addition, we note that the individual factors  $(1 - \frac{1}{\mathbb{N}(P)^s})^{-1}$  are all holomorphic on the region  $\operatorname{Re}(s) > 0$ .

Assume that  $p$  is an unramified prime, that is,  $p \nmid d = \operatorname{disc}(k)$ . (We shall only consider this case, as the ramified primes only contribute a finite number of factors to the product, each of which is holomorphic on the region  $\operatorname{Re}(s) > 0$ . Thus, with respect to questions of convergence, these factors may be ignored.) If  $pA = \prod_{i=1}^N P_i$ , then  $p^n = \prod_{i=1}^N \mathbb{N}(P_i)$ . Thus,  $\prod_{i=1}^N (1 - p^{-f_i s})$  is a polynomial in  $p^{-s}$  of degree  $n$ . If we let  $x = p^{-s}$ , then

$$\prod_{i=1}^N (1 - p^{-f_i s}) = \prod_{i=1}^N (1 - x^{f_i})$$

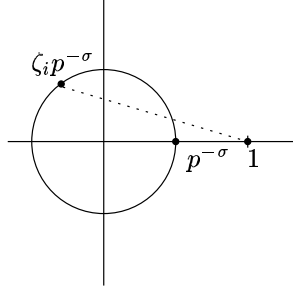
is a polynomial in  $x$  of degree  $n$ . We may factor each  $1 - x^{f_i}$  as  $\prod_{j=1}^{f_i} (1 - \zeta_j x)$  for  $f_i$ th roots of unity  $\zeta_j$ . By renumbering, we see that there are roots of unity  $\zeta_1, \dots, \zeta_n$  such that

$$\prod_{i=1}^N (1 - x^{f_i}) = \prod_{i=1}^n (1 - \zeta_i x)$$

It follows that

$$\prod_{i=1}^N (1 - p^{-f_i s})^{-1} = \prod_{i=1}^n (1 - \zeta_i p^{-s})^{-1}$$

We estimate the size of  $(1 - \zeta_i p^{-s})^{-1}$ . If  $\sigma = \operatorname{Re}(s) > 1$ , then the distance from 1 to  $\zeta_i p^{-s}$  is minimized when  $\zeta_i = 1$ , as the sketch shows.



It follows that

$$\left| \frac{1}{1 - \zeta_i p^{-s}} \right| \leq \frac{1}{1 - p^{-\sigma}}$$

so that

$$\left| \prod_{P|p} \left( 1 - \frac{1}{\mathbb{N}(P)^s} \right)^{-1} \right| \leq ((1 - p^{-\sigma})^{-1})^n$$

and therefore

$$\left| \prod_{p \leq x} \left( \prod_{P|p} \left( 1 - \frac{1}{\mathbb{N}(P)^s} \right)^{-1} \right) \right| \leq \zeta(s)^n$$

as desired.

Next, we wish to understand the nature of the singularity of  $\zeta_k(s)$  at  $s = 1$ . First, recall some notions from the Unit Theorem. Let  $w$  denote the number of roots of unity in  $k$ , so that the group of roots of unity in  $K$  is  $A_{\text{tor}}^\times \cong \mathbb{Z}/w\mathbb{Z}$ . Let  $H$  denote the hyperplane in  $\bigoplus_{v|\infty} \mathbb{R}v$ ,  $H = \{\sum_v a_v v : \sum_v a_v = 0\}$ . We define the map  $\lambda : A^\times \rightarrow H$  as  $\epsilon \mapsto \sum_v \log |\epsilon|_v v$ . Let  $E$  denote the image of  $\lambda$  in  $H$ , which is free of rank  $r = r_1 + r_2 - 1$ . This gives a short exact sequence of abelian groups

$$1 \rightarrow \mathbb{Z}/w\mathbb{Z} \rightarrow A^\times \rightarrow E \rightarrow 1$$

which necessarily splits. Let  $\epsilon_1, \dots, \epsilon_r \in A^\times$  such that the images of the  $\epsilon_i$  in  $E$  form a basis. Then the matrix of  $\lambda$  is

$$M = \begin{pmatrix} \log |\epsilon_1|_{v_1} & \log |\epsilon_2|_{v_1} & \cdots & \log |\epsilon_r|_{v_1} \\ \vdots & \vdots & & \vdots \\ \log |\epsilon_1|_{v_{r+1}} & \log |\epsilon_2|_{v_{r+1}} & \cdots & \log |\epsilon_r|_{v_{r+1}} \end{pmatrix}$$

which is of order  $(r + 1) \times r$ . Let  $M_j$  denote the matrix obtained by deleting the  $j$ th row of  $M$ . We claim that  $|\det(M_j)|$  is independent of  $j$ . To see this, observe that since  $E \subset H$ , the sum of elements of any column of  $M$  is zero. It follows that  $M_j$  is obtained from any  $M_l$  by elementary row operations, so that the determinants differ only up to sign.

**Definition.** With the notation of the previous paragraph, we define the *regulator* of  $k$  as  $R = |\det(M_j)|$ .

There is an equivalent definition of  $R$  which is more geometric. Let  $\mu$  denote the Haar measure on  $H$  induced by the short exact sequence

$$0 \rightarrow H \rightarrow \mathbb{R}^{r+1} \rightarrow \mathbb{R} \rightarrow 0$$

and the normalized Haar measures on  $\mathbb{R}$  and  $\mathbb{R}^{r+1}$ . Let  $G$  be a free abelian subgroup of  $A^\times$  which has finite index  $g$  in  $A^\times$ . It can be shown that

$$\frac{R}{w} = \frac{\mu(H/\lambda(G))}{g}$$

We shall not prove that these definitions are equivalent.

**Theorem 61.** *The function*

$$\zeta_k(s) - \frac{h\kappa}{s-1}$$

*has an analytic continuation to the open half-plane  $\operatorname{Re}(s) > 1 - \frac{1}{n}$  where  $h$  is the class number of  $k$  and*

$$\kappa = \frac{2^{r_1} (2\pi)^{r_2} R}{\sqrt{|d|} w}$$

*In particular,  $\zeta_k(s)$  has a meromorphic extension to this region with unique pole at  $s = 1$  which is simple with residue  $\operatorname{Res}_{s=1} \zeta_k(s) ds = h\kappa$ .*

Below, we offer a sketch of the proof. For a more complete treatment, the interested reader should consult Borevich and Shafarevich *Number Theory*, Chapter 5.

*Sketch of proof.* Let  $C$  denote the ideal class group of  $k$  and fix an ideal class  $c \in C$ . For  $m \in \mathbb{Z}_+$  we define

$$S_c(m) = \#\{I \subseteq A : cl(I) = c \text{ and } \mathbb{N}(I) \leq m\}$$

and

$$S(m) = \sum_{c \in C} S_c(m) = \#\{I \subseteq A : \mathbb{N}(I) \leq m\}$$

The key proposition one proves for this theorem is the following.

**Proposition 62.** *With notation as above*

$$S_c(m) = \kappa m + O(m^{(1-\frac{1}{n})})$$

*In particular, the leading term in the expansion of  $S_c(m)$  is independent of  $c$ .*

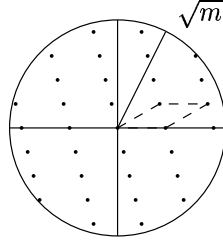
*Sketch of proof in a simple case.* Assume that  $R = 1$ ,  $r_2 = 1$  and  $r_1 = 0$ , so that  $k$  is an imaginary quadratic field. Furthermore, assume that  $c = 1$  in  $C$ . Then

$$S_c(m) = \frac{\#\{\alpha \in A : |\mathbb{N}(\alpha)| \leq m\}}{w}$$

In this computation, we divide by  $w$  because every  $I = \alpha A$  has  $w$  distinct generators, as  $A^\times$  is finite of order  $w$ . If  $\sigma : k \rightarrow \mathbb{C}$  is an embedding, then our assumptions imply that  $\mathbb{N}(\alpha) = \sigma(\alpha)\overline{\sigma(\alpha)}$ . It follows that

$$S_c(m) = \frac{\#\{\alpha \in A : |\sigma(\alpha)| \leq \sqrt{m}\}}{w}$$

The following sketch



leads us to suspect that

$$\#\{\alpha \in A : |\sigma(\alpha)| \leq \sqrt{m}\} \approx \frac{\text{volume of disc}}{\text{volume of fundamental domain for } A} = \frac{\pi m}{\frac{1}{2}|d|^{1/2}}$$

and this estimate is accurate with error  $O(m^{1/2})$ . With this estimate

$$S_c(m) = \frac{2\pi m}{w\sqrt{|d|}} + O(m^{1/2})$$

with our assumptions on  $R$ ,  $r_1$  and  $r_2$  this is exactly the statement

$$S_c(m) = \kappa m + O(m^{(1-\frac{1}{n})})$$

which is the desired conclusion. □

The following is an immediate consequence of Proposition 62.

**Corollary 63.** *With notation as above*

$$S(m) = h\kappa m + O(m^{(1-\frac{1}{n})})$$

The final piece of the puzzle is supplied by a lemma.

**Lemma 64.** *Assume that  $f(s) = \sum_n \frac{b_n}{n^s}$  is a Dirichlet series.*

1. *If  $|b_n| = O(n^{\sigma_0})$ , then the series converges absolutely and defines an analytic function  $f(s)$  on the open half-plane  $\text{Re}(s) > 1 + \sigma_0$ .*
2. *Let  $T(m) = \sum_{n=1}^m b_n$  and suppose that  $|T(m)| = O(m^\sigma)$  for some fixed real number  $\sigma \geq 0$ . Then the Dirichlet series converges and defines a holomorphic function  $f(s)$  in the region  $\text{Re}(s) > \sigma$ . (It will not necessarily converge absolutely in this region.)*

Part 2 of the lemma is more subtle than our previous convergence results, as it is not saying that the series is absolutely convergent. Even though the condition  $|b_n| = O(m^{\sigma_0})$  implies that  $|T(m)| \leq \sum_{n=1}^m |b_n| = O(m^{\sigma_0-1})$ , when we consider conditional convergence, cancellation can occur.

**Example.** Let  $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  be a nontrivial character (i.e., homomorphism of abelian groups). Extend  $\chi$  to a map  $\chi : \mathbb{Z} \rightarrow \mathbb{C}$  by defining  $\chi(n) = 0$  if  $(n, f) \neq 1$ , and consider the Dirichlet series  $\sum_{n=1}^\infty \frac{\chi(n)}{n^s}$ . In the notation of the lemma,  $|b_n| \leq 1$  for all  $n$ , so  $\sigma_0 = 0$  and we have absolute convergence for  $\operatorname{Re}(s) > 1$ . However,  $0 = \sum_{n=1}^f \chi(n) = \sum_{(n,f)=1} \chi(n)$ , so  $|T(m)| = O(1)$  and the original series converges in  $\operatorname{Re}(s) > 0$ , although not absolutely.

*Proof.* We proved part 1 in Lecture 11. For part 2, let  $A_{p,m}$  denote the partial sum

$$A_{p,m} = \sum_{n=p}^m b_n = T(m) - T(p-1)$$

for all  $m > p$ . Then  $|A_{p,m}| = O(m^\sigma)$  because  $m^\sigma \geq (p-1)^\sigma$ . Let  $c_n = n^{-s}$ . Then

$$\begin{aligned} \sum_{n=p}^m b_n n^{-s} &= \sum_{n=p}^m b_n c_n = \sum_{n=p}^m (A_{p,n} - A_{p,n-1}) c_n \\ &= \sum_{n=p}^{m-1} A_{p,n} (c_n - c_{n+1}) + A_{p,m} c_m \\ &= \sum_{n=p}^{m-1} A_{p,n} \left( \frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + A_{p,m} \frac{1}{m^s} \end{aligned}$$

The following bounds

$$\begin{aligned} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| &\leq \frac{|s|}{n^{\operatorname{Re}(s)+1}} \\ |A_{p,n}| &\leq K n^\sigma \\ \left| \frac{A_{p,m}}{m^s} \right| &\leq \frac{K m^\sigma}{m^{\operatorname{Re}(s)}} \end{aligned}$$

imply that

$$\left| \sum_{n=p}^m b_n n^{-s} \right| \leq K \left[ \sum_{n=p}^{m-1} \frac{|s|}{n^{\operatorname{Re}(s)-\sigma+1}} + \frac{1}{m^{\operatorname{Re}(s)-\sigma}} \right]$$

Since  $|s|$  is bounded in any compact region, we see that as  $p, m \rightarrow \infty$  the terms

$$\sum_{n=p}^{m-1} \frac{|s|}{n^{\operatorname{Re}(s)-\sigma+1}} \quad \text{and} \quad \frac{1}{m^{\operatorname{Re}(s)-\sigma}}$$

both tend to zero, by the absolute convergence of  $\zeta(s)$  in the region  $\operatorname{Re}(s) > 1$ . This implies uniform convergence in compact regions, so  $f(s)$  is analytic in  $\operatorname{Re}(s) > \sigma$ , as desired.  $\square$

To see how this completes the proof of the theorem, consider the function

$$f(s) = \zeta_k(s) - h\kappa\zeta(s) = \sum_n \frac{b_n}{n^s}$$

where  $b_n = a_n - h\kappa$ . By Corollary 63 we see that

$$T(m) = \sum_{n=1}^m b_m = (h\kappa m - h\kappa m) + O(m^{(1-\frac{1}{n})})$$

so that Lemma 64 implies that  $f(s)$  is holomorphic on the region  $\text{Re}(s) > 1 - \frac{1}{n}$ . The fact that

$$\zeta_k(s) - \frac{h\kappa}{s-1} = [\zeta_k(s) - h\kappa\zeta(s)] + h\kappa\left[\zeta(s) - \frac{1}{s-1}\right]$$

with Lemma 54 give the desired region of holomorphicity and the correct residue.  $\square$

At the point  $s = 1$  we may consider the formal product

$$\prod_p \left( \prod_{P|p} \left( 1 - \frac{1}{\mathbb{N}(P)} \right)^{-1} \right) = \prod_p \left( \prod_{P|p} \left( \frac{\mathbb{N}(P) - 1}{\mathbb{N}(P)} \right)^{-1} \right) = \prod_p \left( \prod_{P|p} \frac{\mathbb{N}(P)}{\mathbb{N}(P) - 1} \right)$$

obtained by “evaluating”  $\zeta_k(1)$ . If we again disregard the finite number of ramified prime numbers, and consider the factor  $\prod_{\text{char}(P)=p} \frac{\mathbb{N}(P)}{\mathbb{N}(P)-1}$  where  $p \nmid d$ , then we have

$$\prod_{P|p} \frac{\mathbb{N}(P)}{\mathbb{N}(P) - 1} = \frac{p^n}{\prod_{P|p} (\mathbb{N}(P) - 1)} = \frac{p^n}{\prod_{P|p} \#(A/P)^\times} = \frac{p^n}{\#(A/pA)^\times}$$

since the Chinese Remainder Theorem implies that  $A/pA = \prod_{P|p} A/P$ .