Math 105
Supplementary Notes [1]

R. C. Daileda

Introduction

My goal here is to flesh out (more or less completely) some of the arguments presented in our course text [1]. In certain cases this simply means elaborating on the work of the author, while in others (e.g. Hensel's lemma, Ostrowski's theorem) I provide alternate proofs entirely. I plan to update this document throughout the quarter as necessary. Please pass along any typos or suggestions!

II.3

Let R be a DVR with maximal ideal $\mathfrak{p}=\pi R$ and quotient field K. Assume that K is complete with respect to $|\cdot|_{\mathfrak{p}}$, the associated $\mathfrak{p}$-adic absolute value. Given a polynomial $f(x)\in R[x]$, write $\overline{f}(x)$ for the polynomial obtained from f by reducing its coefficients mod $\mathfrak{p}$.

Theorem 1 (Hensel's Lemma). *Let everything be as above. Let $f(x)\in R[x]$ be a monic polynomial and suppose that*

$$\overline{f}(x)=g(x)h(x)$$

for some relatively prime polynomials $g(x),h(x)\in(R/\mathfrak{p})[x]$. Then there exist polynomials $G(x),H(X)\in R[x]$ so that

$$f(x)=G(x)H(x),$$

where $\overline{G}(x)=g(x)$, $\overline{H}(x)=h(x)$ and $\deg G(x)=\deg g(x)$.

Proof. (Taken from [5], pp 129 - 130) For convenience, we omit x from our notation. Let $d=\deg f$, $m=\deg g$. Then, since f is monic, $d-m=\deg h$. We begin by choosing $g_0,h_0\in R[x]$ so that

$$\begin{aligned}\overline{g_0} &= g,\ \deg g_0=\deg g\\ \overline{h_0} &= h,\ \deg h_0=\deg h.\end{aligned}$$

Since g and h are relatively prime in $(R/\mathfrak{p})[x]$, there exist $a,b\in R[x]$ so that

$$ag_0+bh_0\equiv 1 \pmod{\pi}.$$

Our plan is to build $G(x)$ and $H(x)$ through successive approximation. Specifically, we will prove the following:

Claim: There exist $p_i,q_i\in R[x]$, $i\in\mathbb{Z}^+$, so that

$$\begin{aligned}\deg p_i &< m\\ \deg q_i &\leq d-m\end{aligned}$$

and if

$$\begin{aligned}g_n &= g_0+p_1\pi+\cdots+p_n\pi^n\\ h_n &= h_0+q_1\pi+\cdots+q_n\pi^n\end{aligned}$$

then

$$f\equiv g_nh_n \pmod{\pi^{n+1}}$$

[1] Last updated March 6, 2006

for all $n \geq 0$.

If we can establish the claim, then it is clear that the proof of Hensel's lemma will be complete if we set

$$\begin{aligned} G(x) &= \lim_{n\to\infty} g_n(x) \\ H(x) &= \lim_{n\to\infty} h_n(x). \end{aligned}$$

We recursively construct the polynomials p_i, q_i. Note that the final two statements of the claim are true when $n = 0$. So we assume that for some $n \geq 0$ we have found $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_n$ with the desired properties. We seek to define p_{n+1} and q_{n+1}.

Set

$$\begin{aligned} g_{n+1} &= g_n + p_{n+1}\pi^{n+1} \\ h_{n+1} &= h_n + q_{n+1}\pi^{n+1} \end{aligned}$$

where p_{n+1} and q_{n+1} are to be determined. Then

$$\begin{aligned} f &\equiv g_{n+1}h_{n+1} \pmod{\pi^{n+2}} \\ &\Leftrightarrow \\ f - g_n h_n &\equiv (p_{n+1}h_n + q_{n+1}g_n)\pi^{n+1} \pmod{\pi^{n+2}} \\ &\Leftrightarrow \\ f_{n+1} &\equiv p_{n+1}h_0 + q_{n+1}g_0 \pmod{\pi} \end{aligned}$$

where $f_{n+1} = \pi^{-(n+1)}(f - g_n h_n) \in R[x]$. At this point we would like to set $p_{n+1} = bf_{n+1}$, $q_{n+1} = af_{n+1}$. This would satisfy the desired congruence, but the degrees might not be what we want. So we adjust.

Since the leading coefficient of g_0 is a unit in R (otherwise $\deg g_0 < \deg \overline{g_0} = \deg g$), we can write

$$bf_{n+1} = qg_0 + p_{n+1}$$

where $q, p_{n+1} \in R[x]$, $\deg p_{n+1} < \deg g_0 = m$. Then

$$g_0(af_{n+1} + h_0 q) + h_0 p_{n+1} = g_0 a f_{n+1} + h_0 b f_{n+1} \equiv f_{n+1} \pmod{\pi}.$$

We now set

$$q_{n+1} = af_{n+1} + h_0 q - (\text{terms with coefficients divisible by } \pi).$$

Since $\overline{g_0}\,\overline{q_{n+1}} + \overline{h_0}\,\overline{p_{n+1}} = \overline{f_{n+1}}$, $\deg f_{n+1} \leq d$, $\deg h_0 p_{n+1} < d$ and $\deg g_0 = m$, it must be the case that $\deg q_{n+1} = \deg \overline{q_{n+1}} \leq d - m$. Thus, p_{n+1}, q_{n+1} have the desired properties. This proves the claim and hence the theorem. □

The next lemma is an easy consequence of Gauss' lemma from elementary algebra in the case that $R = \mathbb{Z}$, but needs a separate proof in general.

Lemma 1. *Let R be a Dedekind domain with quotient field K. Let $f(x) \in R[x]$ be a monic polynomial and suppose that*

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in K[x]$ monic. Then actually $g(x), h(x) \in R[x]$.

Proof. Since f is monic and $K[x]$ is a UFD we can write

$$f = \prod_{i=1}^{n} p_i^{e_i}$$

where each $p_i \in K[x]$ is irreducible and monic. The roots of f are integral over R and therefore the same is true of the roots of each p_i. Therefore each p_i is the minimal (monic) polynomial over K of an element integral over R. It follows (Proposition I.2.5 of [1]) that $p_i \in R[x]$ for all i. Since g, h are a monic divisors of f, it follows that each is a product of some of the p_i, and therefore $g, h \in R[x]$. □

The following proposition is proven for cyclotomic fields as Proposition I.10.2 in [1]. We use the same proof for the more general version here.

Proposition 1. *Let R be a Dedekind domain with quotient field K of characteristic p. Let β be an mth root of unity, set $L = K(\beta)$ and let R' be the integral closure of R in L. Suppose $p \nmid m$. If a prime $\mathfrak{p}$ of R ramifies in R', then $m \in \mathfrak{p}$.*

Proof. Since $p \nmid m$, the polynomial $x^m - 1$ is separable over K and therefore L/K is a finite separable extension. If $g(x)$ is the minimal polynomial of β over K then $x^m - 1 = g(x)h(x)$, and both $g(x)$ and $h(x)$ have coefficients in R by the lemma. Taking derivatives and evaluating at β gives

$$m\beta^{m-1} = g'(\beta)h(\beta)$$

and taking norms we obtain

$$m^{[L:K]}N_{L/K}(\beta)^{m-1} = N_{L/K}(g'(\beta))N_{L/K}(h(\beta)).$$

By Theorem I.7.6 of [1], $\Delta(\beta) = \pm N_{L/K}(g'(\beta))$. Also, since β is a unit in R', $N_{L/K}(\beta)^{m-1}$ is a unit in R. Finally, since $h(x) \in R[x]$, we have $h(\beta) \in R'$ and so $N_{L/K}(h(\beta)) \in R$. Therefore, passing to ideals in the above gives

$$m^{[L:K]}R \subset \Delta(\beta)R \subset \Delta(R'/R).$$

If $\mathfrak{p}$ ramifies in R' then $\mathfrak{p}$ divides $\Delta(R'/R)$. That is, we have

$$m^{[L:K]}R \subset \Delta(R'/R) \subset \mathfrak{p}.$$

Since $\mathfrak{p}$ is prime, we conclude that $m \in \mathfrak{p}$. □

Now let K be a number field, R the ring of integers in K, $\mathfrak{p}$ a nonzero prime ideal of R and p the positive prime integer in $\mathfrak{p}$. The residue field $R/\mathfrak{p}$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$, with, let's say, $q = p^n$ elements. Let $K_\mathfrak{p}$ denote the completion of K with respect to the $\mathfrak{p}$-adic absolute value. The following is the second half of Theorem II.3.9 of [1].

Theorem 2. *Let β be a primitive $q^f - 1$ root of unity. Then $L = K_\mathfrak{p}(\beta)$ is an unramified extension of $K_\mathfrak{p}$ of degree f.*

Proof. Let $\hat{R}$ be the $\mathfrak{p}$-adic valuation ring in $K_\mathfrak{p}$ and let $\hat{\mathfrak{p}}$ be its maximal ideal. If $\hat{\mathfrak{p}}$ ramifies in L, then according to the proposition above we would have $q^f - 1 \in \hat{\mathfrak{p}}$. This would imply that $q \notin \hat{\mathfrak{p}}$ and hence that $p \notin \hat{\mathfrak{p}}$. But $\hat{\mathfrak{p}} = (\mathfrak{p}R_\mathfrak{p})\hat{R}$ by Theorem II.3.8(a) (or Proposition II.2.4) and $p \in \mathfrak{p}$, which is a contradiction. We conclude that $\hat{\mathfrak{p}}$ is unramified in L, and hence L is an unramified extension of $K_\mathfrak{p}$.

Now we need to compute the degree of L over $K_\mathfrak{p}$. Let $\hat{S}$ denote the integral closure of $\hat{R}$ in L. $\hat{S}$ is a DVR (Theorem II.3.3 of [1]) with unique maximal ideal $\hat{\mathfrak{P}}$. Therefore

$$[L : K_\mathfrak{p}] = e(\hat{\mathfrak{P}}/\hat{\mathfrak{p}})f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}})$$

since L is an unramified extension of $K_\mathfrak{p}$.

We will use Hensel's lemma to show that $f = f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}})$. To simplify notation, set $\kappa = \hat{R}/\hat{\mathfrak{p}}$ and $\kappa' = \hat{S}/\hat{\mathfrak{P}}$. First of all, $x^{q^f-1} - 1$ splits completely in $\hat{S}$. Therefore its reduction $x^{q^f-1} - \overline{1}$ splits into linear factors in κ'. That is, κ' contains the splitting field of $x^{q^f-1} - \overline{1}$, which is a field of q^f elements. It follows that $[\kappa' : \kappa] \geq f$.

Now let $\phi(x) \in \hat{R}[x]$ be the minimal polynomial of β over $K_\mathfrak{p}$. Then $\overline{\phi}(x)$ must be irreducible in $\kappa[x]$ by Hensel's lemma. Therefore

$$[\kappa(\overline{\beta}) : \kappa] = \deg \overline{\phi} = \deg \phi = [L : K_\mathfrak{p}] = f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = [\kappa' : \kappa].$$

So we see that we must have $\kappa' = \kappa(\overline{\beta})$, which means that $\overline{\beta}$ is a primitive $q^{[\kappa':\kappa]} - 1$ root of unity. But $\overline{\beta}$ is also a $q^f - 1$ root of unity, so that $q^{[\kappa':\kappa]} - 1 | q^f - 1$. In particular, $[\kappa' : \kappa] \leq f$.

Putting the results of the previous paragraphs together we have

$$[L : K_\mathfrak{p}] = f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = [\kappa' : \kappa] = f.$$

□

II.4

Here we will provide a proof of the Ostrowski/Gelfand-Tornheim Theorem stated in class. This is for two reasons. First of all, I'm not convinced that one of the steps in the proof in [1] is correct. Secondly, the proof in [5] seems to ignore a slight subtlety, which we will point out below. Our proof will seem somewhat backward when compared to that in [1], since we start with metric vector spaces and move on to theorem afterward.

We define a normed vector space over a valued field as in [1], page 112. We recall the definition for convenience. Let K be a field with valuation $|\cdot|$ and V a vector space over K. A function $||\cdot|| : V \to \mathbb{R}$ is called a *norm* if

1. $||v|| \geq 0$ for all $v \in V$ and $||v|| = 0$ if and only if $v = 0$.
2. $||av|| = |a|\,||v||$ for all $a \in K$ and $v \in V$.
3. $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$.

Notice that the definition of a norm on V is dependent upon the absolute value we are using on K.

Two norms $||\cdot||_1, ||\cdot||_2$ on V are called *equivalent* if there are positive constants C_1 and C_2 so that

$$C_1||v||_1 \leq ||v||_2 \leq C_2||v||_1$$

for all $v \in V$. This is clearly an equivalence relation on the set of all norms of V. The idea here is that equivalent norms define the same metric topology on V.

Lemma 2. *If $|\cdot|$ is an absolute value on a field K and $s \in (0, 1]$, then $|\cdot|_1 = |\cdot|^s$ is an absolute value on K equivalent to $|\cdot|$.*

Proof. We need only prove that $|\cdot|_1$ is an absolute value, since equivalence is clear. $|\cdot|_1$ is clearly multiplicative, nonnegative and zero only at 0. It remains to verify the triangle inequality.

Let $a, x \geq 0$. If $s \in (0, 1]$, then $s - 1 \in (-1, 0]$ and so $(a + x)^{s-1} \leq x^{s-1}$. Integrate from a to $b \geq 0$ to get $(a + b)^s \leq a^s + b^s$. Thus, we have for $x, y \in K$

$$|x + y|_1 = |x + y|^s \leq (|x| + |y|)^s \leq |x|^s + |y|^s = |x|_1 + |y|_1,$$

proving the triangle inequality. □

We can use this to determine all the absolute values on $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) equivalent to the usual one. Indeed, if $|\cdot|_1$ is an absolute value on $\mathbb{R}$ equivalent to the usual, then there is an $s > 0$ so that $|\cdot|_1 = |\cdot|^s$. Then

$$2^s = |2|^s = |2|_1 = |1 + 1|_1 \leq |1|_1 + |1|_1 = 2$$

so that $s \leq 1$. Thus $s \in (0, 1]$. We conclude that all the absolute values on $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) equivalent to the usual are those described in the lemma.

Proposition 2. *Let $|\cdot|_1$ be an absolute value on $\mathbb{R}$ equivalent to the usual one and let V be a finite dimensional vector space over $\mathbb{R}$. All norms on V are equivalent.*

Proof. Fix an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V. For $a_1, \ldots, a_n \in \mathbb{R}$ define

$$\left|\left|\sum_i a_i v_i\right|\right| = \sum_i |a_i|_1.$$

It is trivial to verify that this is a norm. We will show that all norms on V are equivalent to this one. Let $||\cdot||_1$ be any norm on V. Then, given $v \in V$, write $v = \sum_i a_i v_1$, so that

$$||v||_1 \leq \sum_i ||a_i v_1||_1 = \sum_i |a_i|_1\,||v_i||_1 \leq C_2||v||$$

where $C_2 = \max_i ||v_i||_1$. This is half the definition of equivalence. Notice that it proves that the function $v \mapsto ||v||_1$ is continuous with respect to the $||\cdot||$ norm.

For the other half, let $B = \{v \in V : ||v|| = 1\}$. This set is closed and bounded (in $V \cong \mathbb{R}^n$ with the usual Euclidean norm) and so is compact. Therefore the continuous function $v \mapsto ||v||_1$ attains an absolute minimum $C_1 > 0$ on B. Find $s \in (0, 1]$ so that $|\cdot|_1 = |\cdot|^s$, the latter symbol denoting usual absolute value on $\mathbb{R}$. Then for any $v \in V$, $v \neq 0$, we have

$$\left|\left|\frac{v}{||v||^{1/s}}\right|\right| = |||v||^{1/s}|_1^{-1}||v|| = ||v||^{-1}||v|| = 1$$

so that

$$C_1 \leq \left|\left|\frac{v}{||v||^{1/s}}\right|\right|_1 = |||v||^{1/s}|_1^{-1}||v||_1 = ||v||^{-1}||v||_1$$

and hence $C_1||v|| \leq ||v||_1$. □

Corollary 1. *Let $|\cdot|_1 = |\cdot|^s$, $s \in (0, 1]$, be an absolute value on $\mathbb{R}$ equivalent to the usual one. Then $|\cdot|_1$ extends uniquely to $\mathbb{C}$ via the formula $|\cdot|_1 = |\cdot|^s$, the latter being the usual absolute value on $\mathbb{C}$.*

Proof. The formula certainly defines an absolute value on $\mathbb{C}$ equivalent to that given on $\mathbb{R}$. We only need to establish uniqueness. Suppose that $|\cdot|_2$ is another extension. Since $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-vector space, and $|\cdot|_1$, $|\cdot|_2$ are both norms on $\mathbb{C}$, the proposition guarantees the existence of positive constants C_1 and C_2 so that

$$C_1|x|_1 \leq |x|_2 \leq C_2|x|_1$$

for all $x \in \mathbb{C}$. It follows that if $x \neq 0$ then $(|x|_2/|x|_1)^n = |x^n|_2/|x^n|_1 \leq C_2$ for all $n \in \mathbb{Z}$. This can only happen if $|x|_2/|x|_1 = 1$, so we have $|x|_1 = |x|_2$ for all $x \in \mathbb{C}$.

□

We are now ready to prove Ostrowski's theorem as stated in class. While technically complicated, the idea is relatively simple: given a field K complete with respect to an archimedean absolute value, we show that K contains $\mathbb{R}$ and that the absolute value on $\mathbb{R}$ is equivalent to the usual. We then show that $[K : \mathbb{R}] < \infty$ so that $K = \mathbb{R}$ or $K = \mathbb{C}$. The rest will then follow from the corollary above.

Theorem 3. *Let K be a field which is complete with respect to an archimedean valuation $|\cdot|_1$. Then there is an isomorphism $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$ and a real number $s \in (0, 1]$ so that*

$$|x|_1 = |\sigma x|^s$$

for all $x \in K$, the absolute value on the right being the usual absolute value.

Proof. (Taken from [5], pp 124 - 125) Since $|\cdot|_1$ is archimedean, K has characteristic 0 and so contains a copy of $\mathbb{Q}$. Let R be the subfield of K consisting of all limits of Cauchy sequences in $\mathbb{Q}$. It is an easy exercise to see that R is a completion of $\mathbb{Q}$ relative to the restriction of $|\cdot|_1$ to $\mathbb{Q}$. Since $|\cdot|_1$ is archimedean it must be that R is isomorphic to $\mathbb{R}$. Specifically, there exists an isomorphism $\sigma : R \to \mathbb{R}$ over $\mathbb{Q}$ and a real number $s > 0$ so that $|x|_1 = |\sigma x|^s$ for all $x \in R$. Since σ fixes $\mathbb{Q}$, we may argue as above that $s \in (0, 1]$. If $K = R$, we're finished, so assume $K \neq R$.

We claim that every element of K is algebraic over R. Assuming this for the moment, we finish the proof of the theorem. Since $R \cong \mathbb{R}$, and $\mathbb{C}$ is the only nontrivial algebraic extension of $\mathbb{R}$, we conclude that $K \cong \mathbb{C}$. In particular, K is algebraically closed and has degree 2 over R. Choose a root I of $x^2 + 1$ in K. Then $K = R(I)$ and we extend our isomorphism σ to all of K by setting

$$\sigma(a + bI) = \sigma(a) + \sigma(b)i.$$

The formula $|z|_2 = |\sigma^{-1}z|_1$ defines an absolute value on $\mathbb{C}$ which when restricted to $\mathbb{R}$ equals $|\cdot|^s$. By the corollary above, we must have that $|\cdot|_2 = |\cdot|^s$, where the latter absolute value is the usual one on $\mathbb{C}$. Thus, we have an isomorphism $\sigma : K \to \mathbb{C}$ and for any $x \in K$

$$|x|_1 = |\sigma^{-1}\sigma x|_1 = |\sigma x|_2 = |\sigma x|^s.$$

Therefore, it only remains to prove our claim that K is algebraic over R. We will, in fact, show that every $\xi \in K \setminus R$ is of degree 2 over R. Define $f : \mathbb{C} \to \mathbb{R}$ by

$$f(z) = |\xi^2 - \sigma^{-1}(z + \overline{z})\xi + \sigma^{-1}(z\overline{z})|_1.$$

It is straightforward to verify that this is continuous and satisfies $\lim_{z\to\infty} f(z) = \infty$. Therefore it assumes its minimum m and the set

$$S = \{z \in \mathbb{C} : f(z) = m\}$$

is nonempty, bounded and closed. Hence there is a $z_0 \in S$ so that $|z_0| \geq |z|$ for all $z \in S$.

It is sufficient to show that $m = 0$. Assume otherwise. Then $m > 0$. Consider the real polynomial

$$g(x) = x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 + \epsilon$$

for some $0 < \epsilon < m^{1/s}$. It has roots $z_1, \overline{z}_1 \in \mathbb{C}$ which satisfy $z_1\overline{z}_1 = z_0\overline{z}_0 + \epsilon$, so that $|z_1| > |z_0|$. Hence $z_1 \notin S$ and $f(z_1) > m$. Now consider the real polynomial

$$G(x) = (g(x) - \epsilon)^n - (-\epsilon)^n = \prod_{i=1}^{2n}(x - \alpha_i) = \prod_{i=1}^{2n}(x - \overline{\alpha}_i)$$

with roots $\alpha_1, \ldots, \alpha_2 n \in \mathbb{C}$. Since $G(z_1) = 0$ we may assume that $z_1 = \alpha_1$. Notice that

$$G(x)^2 = \prod_{i=1}^{2n}\left(x^2 - (\alpha_i + \overline{\alpha}_i)x + \alpha_i\overline{\alpha}_i\right),$$

the factors on the right having real coefficients. Extending σ to an isomorphism $R[x] \to \mathbb{R}[x]$ in the usual way, we have

$$\left|(\sigma^{-1}G)(\xi)\right|_1^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(z_1)m^{2n-1}$$

and

$$\begin{aligned}
\left|(\sigma^{-1}G)(\xi)\right|_1 &= \left|\left(\xi^2 - \sigma^{-1}(z_0 + \overline{z}_0)\xi + \sigma^{-1}(z_0\overline{z}_0)\right)^n - \sigma^{-1}(-\epsilon)^n\right|_1 \\
&\leq f(z_0)^n + \left|\sigma^{-1}(\epsilon)\right|_1^n \\
&= f(z_0)^n + \epsilon^{ns} \\
&= m^n + \epsilon^{ns}
\end{aligned}$$

It follows that $f(z_1)m^{2n-1} \leq (m^n + \epsilon^{ns})^2$ and hence

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\epsilon^s}{m}\right)^n\right)^2.$$

Letting $n \to \infty$ gives $f(z_1) \leq m$, which is a contradiction.

□

Corollary 2. *Let K be a field complete with respect to a nonarchimedean absolute value and let L be a finite extension. The absolute value on K extends uniquely to L, and L is complete with respect to this extension.*

Proof. Let $|\cdot|_1$ be the absolute value on K, $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$ be the isomorphism and $s \in (0, 1]$ the exponent of the preceding theorem. There is nothing to prove if $K = L$, so we can assume that the image of the isomorphism is $\mathbb{R}$ and $K \neq L$. It follows that L is isomorphic to $\mathbb{C}$, contains a root I of $x^2 + 1$ and $L = K(I)$. As above, σ extends to an isomorphism $\sigma : L \to \mathbb{C}$ via

$$\sigma(a + bI) = \sigma(a) + \sigma(b)i.$$

The function $|x|_2 = |\sigma x|^s$ is an absolute value on L, equal to $|\cdot|_1$ on K. It is clear that the completeness of $\mathbb{C}$ now implies the completeness of L relative to this extended absolute value. That $|\cdot|_2$ is the only extension of $|\cdot|_1$ to L follows from the preceding corollary, since any other extension, in conjunction with σ, can be used to give an extension of $|\cdot|^s$ to all of $\mathbb{C}$. □

Corollary 3. *Let K be a number field and let $|\cdot|_1$ be an archimedean absolute value on K. Then there is an embedding σ of K into $\mathbb{R}$ or $\mathbb{C}$ and a real number $s \in (0,1]$ so that*

$$|x|_1 = |\sigma x|^s$$

for all $x \in K$.

Proof. Let $\hat{K}$ denote the completion of K with respect to $|\cdot|_1$. By the theorem, there is an $s \in (0,1]$ and an isomorphism σ of $\hat{K}$ with $\mathbb{R}$ or $\mathbb{C}$ so that $|x|_1 = |\sigma x|^s$ for all $x \in \hat{K}$. The result follows by simply restricting σ to K. □

II.5

Theorem 4. *Let K be a number field and $\mathfrak{p}$ a prime of K. Let L be a finite extension of K. Then there is an isomorphism (as both $K_\mathfrak{p}$- and L-algebras)*

$$K_\mathfrak{p} \otimes_K L \cong \sum_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$$

where the direct sum runs over the primes of L extending $\mathfrak{p}$.

Proof. This is just an expanded version of the proof given in [1]. Let $\mathfrak{P}$ be a prime of L extending $\mathfrak{p}$. We choose valuations $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{P}$ in $\mathfrak{p}$ and $\mathfrak{P}$, respectively, so that $|x|_\mathfrak{p} = |x|_\mathfrak{P}$ for all $x \in K$. Let $K_\mathfrak{p}$ and $L_\mathfrak{P}$ be the associated completions and assume that $K \subset K_\mathfrak{p}$, $L \subset L_\mathfrak{P}$. According to Theorem II.2.2 of [1], there is a commutative diagram

$$\begin{array}{ccc} K & \longrightarrow & L \\ \downarrow & & \downarrow \\ K_\mathfrak{p} & \xrightarrow[\sigma_\mathfrak{P}]{} & L_\mathfrak{P} \end{array}$$

in which the unlabeled arrows are inclusions and all maps preserve absolute values. We use the map $\sigma_\mathfrak{P}$ to make $L_\mathfrak{P}$ into a $K_\mathfrak{p}$-algebra.

Through the usual abstract nonsense regarding maps out of tensor products, there is a well-defined map $K_\mathfrak{p} \otimes_K L \to L_\mathfrak{P}$ satisfying

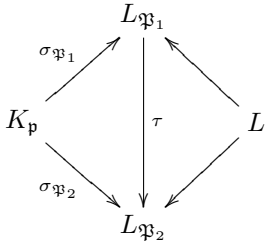
$$\alpha \otimes x \mapsto \sigma_\mathfrak{P}(\alpha)x.$$

It is easy to see that this is both a $K_\mathfrak{p}$- and L-algebra homomorphism. We claim that it is surjective. Let $a_1, \ldots, a_n$ be a K-basis for L. Let $M = \sigma_\mathfrak{P}(K_\mathfrak{p})[a_1, \ldots, a_n]$. This is a subfield of $L_\mathfrak{P}$ which contains K and $a_1, \ldots, a_n$. Hence $L \subset M$. Moreover, M is clearly finite dimensional over the complete field $\sigma_\mathfrak{P}(K_\mathfrak{p})$ and so $|\cdot|_\mathfrak{P}$ is the unique extension of the absolute value on $\sigma_\mathfrak{P}(K_\mathfrak{p})$ to M. Therefore, M contains L and is complete with respect to the absolute value $|\cdot|_\mathfrak{P}$. It follows that every Cauchy sequence in L actually converges in M, and so $L_\mathfrak{P} = M = \sigma_\mathfrak{P}(K_\mathfrak{p})[a_1, \ldots, a_n]$. This shows that the elements $1 \otimes a_i$ of $K_\mathfrak{p} \otimes_K L$ map to $K_\mathfrak{p}$-generators of $L_\mathfrak{P}$, which proves surjectivity.

Now let $M_\mathfrak{P}$ be the kernel of the map $K_\mathfrak{p} \otimes_K L \to L_\mathfrak{P}$. As $L_\mathfrak{P}$ is a field, $M_\mathfrak{P}$ is maximal. In fact, if $\mathfrak{P}_1 \neq \mathfrak{P}_2$ both extend $\mathfrak{p}$, then $M_{\mathfrak{P}_1}$ and $M_{\mathfrak{P}_2}$ are distinct. To see this, suppose the contrary holds. Then $M_{\mathfrak{P}_1} = M_{\mathfrak{P}_2}$ and factoring through the maps above gives isomorphisms

$$L_{\mathfrak{P}_1} \cong K_\mathfrak{p} \otimes_K L/M_{\mathfrak{P}_1} = K_\mathfrak{p} \otimes_K L/M_{\mathfrak{P}_2} \cong L_{\mathfrak{P}_2}.$$

Denote the composite isomorphism by τ. Using the definitions we have given, it is not hard to see that the diagram



commutes, where the unlabeled maps are inclusions. For $x \in L_{\mathfrak{P}_1}$ set $|x|_1 = |\tau x|_{\mathfrak{P}_2}$. This is an absolute value on $L_{\mathfrak{P}_1}$. For $x \in K_{\mathfrak{p}}$ we have

$$|\sigma_{\mathfrak{P}_1} x|_{\mathfrak{P}_1} = |x|_{\mathfrak{p}} = |\sigma_{\mathfrak{P}_2} x|_{\mathfrak{P}_2} = |\tau\sigma_{\mathfrak{P}_1} x|_{\mathfrak{P}_2} = |\sigma_{\mathfrak{P}_1} x|_1.$$

Therefore both $|\cdot|_{\mathfrak{P}_1}$ and $|\cdot|_1$ extend the absolute value on the complete field $\sigma_{\mathfrak{P}_1}(K_{\mathfrak{p}})$ to all of $L_{\mathfrak{P}_1}$. Since such an extension is unique, it follows that $|x|_{\mathfrak{P}_1} = |x|_1$ for all $x \in L_{\mathfrak{P}_1}$. In particular, for $x \in L$ we have

$$|x|_{\mathfrak{P}_1} = |x|_1 = |\tau x|_{\mathfrak{P}_2} = |x|_{\mathfrak{P}_2}$$

since τ fixes L by commutativity of the diagram above. That is, $|\cdot|_{\mathfrak{P}_1}$ and $|\cdot|_{\mathfrak{P}_2}$ are equivalent, contradicting $\mathfrak{P}_1 \neq \mathfrak{P}_2$.

We are almost finished. Since the maximal ideals $M_{\mathfrak{P}}$ are distinct for distinct $\mathfrak{P}|\mathfrak{p}$, the Chinese remainder theorem gives a surjective ring homomorphism

$$K_{\mathfrak{p}} \otimes_K L \to \sum_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{p}} \otimes_K L/M_{\mathfrak{P}} \cong \sum_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}},$$

the isomorphism on the right being the sum of those described above. Once again, it is easy to verify that this is both a $K_{\mathfrak{p}}$- and L-algebra homomorphism. Finally, we notice that

$$\dim_{K_{\mathfrak{p}}} K_{\mathfrak{p}} \otimes_K L = \dim_K L = [L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = \dim_{K_{\mathfrak{p}}} \sum_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}.$$

Equality of dimensions implies the surjection is actually an isomorphism, and the theorem is proved. □

III.1

The notes for this section cover almost every result in section III.1 of [1]. As such, this section is a little lengthier than the rest. At the outset, these notes are somewhat different than what is presented in [1]. We work a little more generally, with the benefit being a few (dramatically!) simplified proofs. We then move on to statements and (elaborated) proofs as given in the text.

Let L/K be a Galois extension of number fields with group $G = G(L/K)$. Let $\mathfrak{p}$ be a prime of K (finite or infinite) and let $\mathfrak{P}$ be a prime of L, $\mathfrak{P}|\mathfrak{p}$. We will call this set of conditions/notation the *usual hypotheses* throughout this section. Let $S(\mathfrak{p})$ denote the set of primes of L that divide $\mathfrak{p}$.

We can define an action of G on $S(\mathfrak{p})$ as follows. Let $\mathfrak{P} \in S(\mathfrak{p})$, $\sigma \in G$. Choose a representative $|\cdot| \in \mathfrak{P}$. Define a new absolute value $|\cdot|^\sigma$ on L by the formula

$$|x|^\sigma = |\sigma^{-1} x|$$

for all $x \in L$. Let $\sigma\mathfrak{P}$ denote the prime of L containing $|\cdot|^\sigma$. Since σ fixes K, $|\cdot|^\sigma$ and $|\cdot|$ both agree on K, and since $|\cdot|$ extends the absolute values of $\mathfrak{p}$ we conclude that the same holds for $|\cdot|^\sigma$. Thus $\sigma\mathfrak{P}|\mathfrak{p}$, or $\sigma\mathfrak{P} \in S(\mathfrak{p})$. It is straightforward to verify that the definition of $\sigma\mathfrak{P}$ does not depend on the representative we choose, so our notation is unambiguous. Once this verification has been made, it is equally easy verify that the assignment $\mathfrak{P} \mapsto \sigma\mathfrak{P}$ gives a bona-fide group action of G on $S(\mathfrak{p})$.

Before studying this action more closely, let's choose some convenient representatives of our primes. Let $\mathfrak{p}$ be a prime of K. If $\mathfrak{p}$ is finite view it as a prime ideal in K, choose some $c \in (0, 1)$ and set $|x|_{\mathfrak{p}} = c^{\nu_{\mathfrak{p}}(x)}$ for all $x \in K$. A prime $\mathfrak{P}$ of L over K can also be viewed as a prime ideal (this time of L) and we set $|x|_{\mathfrak{P}} = c_{\mathfrak{P}}^{\nu_{\mathfrak{P}}(x)}$ where $c_{\mathfrak{P}} = c^{1/e(\mathfrak{P}/\mathfrak{p})}$. If $\mathfrak{p}$ is infinite, then $\mathfrak{p}$ corresponds to an embedding $\tau : K \to \mathbb{R}$ or $\mathbb{C}$. We set $|x|_{\mathfrak{p}} = |\tau x|_{\mathbb{C}}$ for $x \in K$. An extensions $\mathfrak{P}|\mathfrak{p}$ of $\mathfrak{p}$ to L is given by a lift $\hat{\tau}$ of τ to L, and we set $|x|_{\mathfrak{P}} = |\hat{\tau} x|_{\mathbb{C}}$ for $x \in L$.

The upshot of the preceding paragraph is that for each prime $\mathfrak{p}$ of K and prime $\mathfrak{P}$ of L with $\mathfrak{P}|\mathfrak{p}$ we have representative absolute values $|\cdot|_{\mathfrak{p}} \in \mathfrak{p}$ and $|\cdot|_{\mathfrak{P}} \in \mathfrak{P}$ that satisfy

$$|x|_{\mathfrak{p}} = |x|_{\mathfrak{P}} \tag{1}$$

for all $x \in K$ and all $\mathfrak{P}|\mathfrak{p}$. For infinite primes this is immediate from our definitions, whereas for finite primes it follows from the fact that if $\mathfrak{P}|\mathfrak{p}$ then $\nu_{\mathfrak{P}}(x) = e(\mathfrak{P}/\mathfrak{p})\nu_{\mathfrak{p}}(x)$ for $x \in K$.

Why have we made these choices? Because equation (1) allows us to conclude that the action of G actually maps these representatives to one another. To see this, let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ be a prime of L with $\mathfrak{P}|\mathfrak{p}$. By equation (1) we have for $x \in K$:

$$|x|_{\sigma\mathfrak{P}} = |x|_{\mathfrak{p}} = |\sigma^{-1}x|_{\mathfrak{p}} = |\sigma^{-1}x|_{\mathfrak{P}} = |x|_{\mathfrak{P}}^{\sigma}.$$

Moreover, $|\cdot|_{\sigma\mathfrak{P}}$ and $|\cdot|_{\mathfrak{P}}^{\sigma}$ are equivalent by the definition of $\sigma\mathfrak{P}$. Since they agree on K, equivalence forces that they must actually agree on all of L (use Proposition II.1.1 of [1]). That is

$$|x|_{\sigma\mathfrak{P}} = |x|_{\mathfrak{P}}^{\sigma} \tag{2}$$

for all $x \in L$.

We know that the primes of a number field K arise from other more explicit objects associated with K, namely prime ideals and embeddings. Using the normalized representatives of the primes that we've just described, we can interpret the action of G on $S(\mathfrak{p})$ for a given prime $\mathfrak{p}$ of K in terms of these explicit objects.

We begin with finite primes. A finite prime $\mathfrak{p}$ of K corresponds to a primie ideal of K which we denote by $\mathfrak{p}$ as well. The primes $\mathfrak{P}|\mathfrak{p}$ of L correspond to prime ideals of L which contain $\mathfrak{P}$. We denote these by $\mathfrak{P}$ as well. The Galois group G acts on the prime ideals $\mathfrak{P}$ over $\mathfrak{p}$: if $\sigma \in G$ and $\mathfrak{P}$ lies over $\mathfrak{p}$ in L, then $\sigma(\mathfrak{P})$ (σ applied element-wise to $\mathfrak{P}$) is also a prime ideal lying over $\mathfrak{p}$. We clearly have $\nu_{\mathfrak{P}}(\sigma^{-1}x) = \nu_{\sigma(\mathfrak{P})}(x)$ for $x \in L$, which implies that $|\cdot|_{\mathfrak{P}}^{\sigma}$ and $|\cdot|_{\sigma(\mathfrak{P})}$ are equivalent. However, according to how we've normalized things, these absolute values both equal $|\cdot|_{\mathfrak{p}}$ on K. As before, this condition together with equivalence implies the absolute values are actually identical on L. Thus, we have

$$|x|_{\sigma\mathfrak{P}} = |x|_{\mathfrak{P}}^{\sigma} = |x|_{\sigma(\mathfrak{P})}$$

for all$x \in L$. This shows that under our correspondence between finite primes of L and prime ideals of L, the *equivalence class* $\sigma\mathfrak{P}$ corresponds to the *prime ideal* $\sigma(\mathfrak{P})$. We encapsulate our work in the next lemma.

Lemma 3. *Given the usual hypotheses, with $\mathfrak{p}$ a finite prime of K, the correspondence between finite primes of L extending $\mathfrak{p}$ and prime ideals of L lying over the prime ideal corresponding to $\mathfrak{p}$ respects the action of the group G.*

We now seek to prove the analogous statement for an infinite prime $\mathfrak{p}$ of K. So, suppose that $\mathfrak{p}$ corresponds to the embedding τ of K (into $\mathbb{R}$ or $\mathbb{C}$). We know that the primes $\mathfrak{P}$ of L extending $\mathfrak{p}$ correspond to the non-conjugate lifts of τ to an embedding of L. The group G acts on these lifts. If $\sigma \in G$ and $\hat{\tau}$ is a lift of τ then $\hat{\tau}\sigma^{-1}$ is also a lift of τ. Moreover, if $\mathfrak{P}$ is the prime corresponding to $\hat{\tau}$ then

$$|x|_{\sigma\mathfrak{P}} = |x|_{\mathfrak{P}}^{\sigma} = |\sigma^{-1}x|_{\mathfrak{P}} = |\hat{\tau}\sigma^{-1}x|_{\mathbb{C}}$$

for all $x \in L$. This tells us that $\sigma\mathfrak{P}$ is the prime corresponding to the embedding $\hat{\tau}\sigma^{-1}$. So, under the correspondence between infinite primes of L and embeddings of L, the *equivalence class* $\sigma\mathfrak{P}$ corresponds to the *embedding* $\hat{\tau}\sigma^{-1}$. Again, we summarize.

Lemma 4. *Given the usual hypotheses, with $\mathfrak{p}$ and infinite prime of K, the correspondence between infinite primes of L extending $\mathfrak{p}$ and the embeddings of L lifting the embedding corresponding to $\mathfrak{p}$ respects the action of the group G.*

These lemmas now let us make our first observation about the action of G on primes.

Theorem 5. *Given the usual hypotheses, for $\sigma \in G$, $\mathfrak{P}|\mathfrak{p}$, the rule $\mathfrak{P} \mapsto \sigma\mathfrak{P}$ defines a transitive action of G on the set of primes of L extending $\mathfrak{p}$.*

Proof. We only need to establish transitivity. If $\mathfrak{p}$ is finite, then it is a standard result that G transitively permutes the prime ideals of L over $\mathfrak{p}$. The conclusion of the theorem then follows from Lemma 3. If $\mathfrak{p}$ is infinite, corresponding to the embedding τ of K, then by Lemma 4 it is enough to show that G acts transitively on the lifts of τ to L. If $\hat{\tau}$ is any such lift, then $\hat{\tau}\sigma^{-1}$, $\sigma \in G$, gives $|G| = [L : K]$ distinct lifts of τ to L. But τ only has $[L : K]$ lifts, so we must get them all in this manner. This proves transitivity of G on lifts of τ. □

Proposition 3. *Given the usual hypotheses, the numbers $e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p})$ are the same for all $\mathfrak{P}|\mathfrak{p}$.*

Proof. For finite primes this is a standard result for Galois extensions of number fields. If $\mathfrak{p}$ is infinite then $f(\mathfrak{P}|\mathfrak{p}) = 1$ for all $\mathfrak{P}|\mathfrak{p}$ by definition, so there is nothing to prove about the inertia numbers. As we have just seen, G acts transitively on the lifts of any given embedding of K. It follows that if a single lift has real (resp. complex) image, then *every* lift has real (resp. complex) image. From this it follows that $e(\mathfrak{P}/\mathfrak{p}) = 1$ for every $\mathfrak{P}|\mathfrak{p}$ or $e(\mathfrak{P}/\mathfrak{p}) = 2$ for every $\mathfrak{P}|\mathfrak{p}$. □

Given the usual hypotheses, the *decomposition group* of $\mathfrak{P}$ is defined to be

$$G(\mathfrak{P}) = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\} = \mathrm{Stab}_G(\mathfrak{P}).$$

The theorem and proposition above give us one immediate fact about $G(\mathfrak{P})$.

Theorem 6. *Given the usual hypotheses, we have*

$$|G(\mathfrak{P})| = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

Proof. Since the action of G on $S(\mathfrak{p})$ is transitive, the G-orbit of $\mathfrak{P}$ is all of $S(\mathfrak{p})$. Since $G(\mathfrak{P})$ is the stabilizer of $\mathfrak{P}$ in G, it follows that

$$|S(\mathfrak{p})| = [G : G(\mathfrak{P})] = \frac{|G|}{|G(\mathfrak{P})|} = \frac{[L : K]}{|G(\mathfrak{P})|}.$$

Write the factorization of $\mathfrak{p}$ in L as

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

and let $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. The proposition tells us that all of the e_i and f_i are the same so that

$$[L : K] = \sum_{i=1}^{g} e_i f_i = ge(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/p) = |S(\mathfrak{p})|e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$$

and the result follows. □

Once again we need to fix our notation. Given the usual hypotheses, fix a completion $L_{\mathfrak{P}}$ of L at $\mathfrak{P}$, relative to the representative $|\cdot|_{\mathfrak{P}}$ chosen above. Using the usual fact (Theorem II.2.2 of [1]) we know we can embed (in a unique way) the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$ with respect to $|\cdot|_{\mathfrak{p}}$ inside $L_{\mathfrak{P}}$. Using this embedding, we can treat K, L and $K_{\mathfrak{p}}$ as *subfields* of $L_{\mathfrak{P}}$, the absolute value $|\cdot|_{\mathfrak{P}}$ on $L_{\mathfrak{P}}$ restricting to give the appropriate absolute values on K, L and $K_{\mathfrak{P}}$.

Lemma 5. *There is an injective homomorphism*

$$\begin{array}{ccc} G(\mathfrak{P}) & \to & Aut_{K_{\mathfrak{p}}}(L_{\mathfrak{P}}) \\ \sigma & \mapsto & \hat{\sigma} \end{array}$$

satisfying $\hat{\sigma}|_L = \sigma$.

Proof. For $\sigma \in G(\mathfrak{P})$ and $x \in L$ we have

$$|\sigma x|_{\mathfrak{P}} = |\sigma x|_{\sigma\mathfrak{P}} = |\sigma x|_{\mathfrak{P}}^{\sigma} = |\sigma^{-1}\sigma x|_{\mathfrak{P}} = |x|_{\mathfrak{P}}$$

so that σ preserves the absolute value $|\cdot|_{\mathfrak{P}}$. The usual result (Theorem II.2.2 of [1] again) gives us a unique lift $\hat{\sigma}$ so that

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ \downarrow & & \downarrow \\ L_{\mathfrak{P}} & \xrightarrow{\hat{\sigma}} & L_{\mathfrak{P}} \end{array}$$

commutes and absolute values are preserved. If $\sigma, \tau \in G(\mathfrak{P})$ then the composition $\hat{\sigma}\hat{\tau}$ provides a lift of $\sigma\tau$ that preserves absolute values. The uniqueness statement of Theorem II.2.2 then implies that $\widehat{\sigma\tau} = \hat{\sigma}\hat{\tau}$, so

we do indeed have a homomorphism. That $\hat{\sigma}|_L = \sigma$ follows from the diagram, and this implies injectivity of the map.

It remains to show that $\hat{\sigma}$ fixes $K_{\mathfrak{p}}$. Since $\hat{\sigma}$ preserves absolute values, it is easy to see that if the sequence $a_n \in L_{\mathfrak{P}}$ converges to $a \in L_{\mathfrak{P}}$ then $\hat{\sigma}a_n \to \hat{\sigma}a$. Let $a \in K_{\mathfrak{p}}$ and choose a sequence $a_n \in K$ so that $a_n \to a$. Since σ fixes K we have

$$\hat{\sigma}a = \lim_{n\to\infty} \hat{\sigma}a_n = \lim_{n\to\infty} \sigma a_n = \lim_{n\to\infty} a_n = a$$

so that $\hat{\sigma}$ does indeed fix $K_{\mathfrak{p}}$. □

We can now deduce a second fact about decomposition groups. To keep our notation simple, we use the homomorphism just described to view $G(\mathfrak{P})$ as a group of $K_{\mathfrak{p}}$-automorphisms of $L_{\mathfrak{P}}$.

Theorem 7. *Given the usual hypotheses, the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois with group $G(\mathfrak{P})$.*

Proof. Let E be the subfield of $L_{\mathfrak{P}}$ fixed by $G(\mathfrak{P})$. Then $L_{\mathfrak{P}}/E$ is Galois with group $G(\mathfrak{P})$. We clearly have $K_{\mathfrak{p}} \subset E$ so that

$$e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L : E][E : K_{\mathfrak{p}}] = |G(\mathfrak{P})|[E : K_{\mathfrak{p}}] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})[E : K_{\mathfrak{p}}]$$

which implies that $[E : K_{\mathfrak{p}}] = 1$. Hence $E = K_{\mathfrak{p}}$ and the theorem is proved. □

This theorem and its predecessor are given as Theorem III.1.2 and Corollary III.1.3 in [1]. Here we have provided entirely different proofs based on elementary facts about group actions.

Having studied the relationship between decomposition groups and completions (via liftings), we now study of the relationship of decomposition groups and residue fields (via quotients). This will lead us to inertia groups. Once again, we invoke the usual hypotheses, but now we require $\mathfrak{p}$ to be a finite prime, which we identify with a prime ideal in K. We let R be the ring of integers in F and we let R' denote the ring of integers in K. We let $\mathfrak{P}$ denote a prime of R' lying over $\mathfrak{p}$. We denote the residue fields $R/\mathfrak{P}$ and $R'/\mathfrak{P}$ by $\bar{R}$ and $\bar{R}'$, respectively.

Lemma 6. *There is a homomorphism*

$$\begin{array}{ccc} G(\mathfrak{P}) & \to & G(\bar{R}'/\bar{R}) \\ \sigma & \mapsto & \bar{\sigma} \end{array}$$

where $\bar{\sigma}$ is defined by

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$$

for all $x \in R'$.

Proof. For $\sigma \in G(\mathfrak{P})$ we have $\sigma(\mathfrak{P}) = \mathfrak{P}$. This implies that $\bar{\sigma}$ is well-defined. Since σ fixes R, it follows that $\bar{\sigma}$ fixes $\bar{R}$. The rest is trivial. □

The kernel of the homomorphism of Lemma 6 is called the *inertia group* of $\mathfrak{P}$ and we denote it by $T(\mathfrak{P})$. Our goal is to prove Theorem 8 below. In order to do this carefully we need a few somewhat tedious, but elementary, lemmas.

We start by passing to completions. Let $\hat{R}$, $\hat{R}'$ denote the valuation rings in the completions $K_{\mathfrak{p}}$, $L_{\mathfrak{P}}$ (resp.) and let $\hat{P}$, $\hat{\mathfrak{P}}$ denote the corresponding maximal ideals. We know that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois with group (isomorphic to) $G(\mathfrak{p})$. As above, we use the overline $\bar{}$ to denote passage to the residue fields. We prove the analogue of Lemma 6.

Lemma 7. *There is a homomorphism*

$$\begin{array}{ccc} G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) & \to & G\left(\bar{\hat{R}}'/\bar{\hat{R}}\right) \\ \sigma & \mapsto & \bar{\sigma} \end{array}$$

where $\bar{\sigma}$ is defined by

$$\bar{\sigma}(x + \hat{\mathfrak{P}}) = \sigma(x) + \hat{\mathfrak{P}}$$

Proof. Let $\sigma \in G(L_{\hat{\mathfrak{P}}}/K_{\mathfrak{p}})$. We know that $\hat{R}'$ is the integral closure of $\hat{R}$ in $L_{\hat{\mathfrak{P}}}$. Since $\sigma \in G(L_{\hat{\mathfrak{P}}}/K_{\mathfrak{p}})$ fixes $K_{\mathfrak{p}}$, is must map $\hat{R}'$ onto itself. Furthermore, σ maps prime ideals of $\hat{R}'$ to prime ideals. Since $\hat{\mathfrak{P}}$ is the only prime in $\hat{R}'$, it follows that $\sigma(\hat{\mathfrak{P}}) = \hat{\mathfrak{P}}$. The rest of the proof is the same as that for Lemma 6. □

Since the Galois group $G(L_{\hat{\mathfrak{P}}}/K_{\mathfrak{p}})$ is isomorphic to $G(\mathfrak{P})$ in a natural way, and the residue fields are all isomorphic in a natural way, it shouldn't be surprising to learn that the lemma we've just proved and Lemma 6 both have the same content. This is the point of the next lemma.

Lemma 8. *There is a commutative diagram*

$$\begin{array}{ccc} G(\mathfrak{P}) & \xrightarrow[\sim]{\widehat{\ }} & G(L_{\hat{\mathfrak{P}}}/K_{\mathfrak{p}}) \\ - \downarrow & & - \downarrow \\ G(\bar{R}'/\bar{R}) & \xrightarrow[\sim]{\widehat{\ }} & G(\bar{\hat{R}}'/\bar{\hat{R}}) \end{array}$$

all maps aside from the bottom being those defined earlier.

Proof. We need to define the bottom map and then verify commutativity. We know that inclusion induces isomorphisms

$$\bar{R}' = R'/\mathfrak{P} \cong R'_{\mathfrak{P}}/\mathfrak{P}R'_{\mathfrak{P}} \cong \hat{R}'/\hat{\mathfrak{P}} = \bar{\hat{R}}'$$

and we denote the composite isomorphism (from left to right) by ι. Likewise, inclusion gives us the isomorphisms

$$\bar{R} = R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \hat{R}/\hat{\mathfrak{p}} = \bar{\hat{R}}$$

and these are compatible with the inclusions $R/\mathfrak{p} \hookrightarrow R'/\mathfrak{P}$ and $\hat{R}/\hat{\mathfrak{p}} \hookrightarrow \hat{R}'/\hat{\mathfrak{P}}$. We define the map $G(\bar{R}'/\bar{R}) \to G(\bar{\hat{R}}'/\bar{\hat{R}})$ by

$$\sigma \mapsto \hat{\sigma} = \iota\sigma\iota^{-1}.$$

This is clearly an injective homomorphism. Since $f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = f(\mathfrak{P}/\mathfrak{p})$, both groups have the same size and the map is thus an isomorphism.

Now on to commutativity. Given $\sigma \in G(\mathfrak{P})$ we need to show that

$$\hat{\bar{\sigma}} = \bar{\hat{\sigma}}.$$

Let $x \in \hat{R}'$. Choose $y \in R'$ so that $y + \hat{\mathfrak{P}} = \iota(y + \mathfrak{P}) = x + \hat{\mathfrak{P}}$. Then $x - y \in \hat{\mathfrak{P}}$. Thus

$$\hat{\sigma}x - \hat{\sigma}y = \hat{\sigma}(x - y) \in \hat{\sigma}(\hat{\mathfrak{P}}) = \hat{\mathfrak{P}}.$$

The fact that $\hat{\sigma}(\hat{\mathfrak{P}}) = \hat{\mathfrak{P}}$ was proven earlier. Since $y \in L$, $\hat{\sigma}y = \sigma y$. We thus conclude that $\hat{\sigma}x + \hat{\mathfrak{P}} = \sigma y + \hat{\mathfrak{P}}$. So, finally,

$$\begin{aligned} \hat{\bar{\sigma}}(x + \hat{\mathfrak{P}}) &= \iota\bar{\sigma}\iota^{-1}(x + \hat{\mathfrak{P}}) \\ &= \iota\bar{\sigma}(y + \mathfrak{P}) \\ &= \iota(\sigma y + \mathfrak{P}) \\ &= \sigma y + \hat{\mathfrak{P}} \\ &= \hat{\sigma}x + \hat{\mathfrak{P}} \\ &= \bar{\hat{\sigma}}(x + \hat{\mathfrak{P}}). \end{aligned}$$

This is what we needed to show. □

After these technicalities, we can now state and prove (carefully!) the result that we're really after. Our proof is essentially that given in [1], we've just fleshed out the details.

Theorem 8. *Let everything be as above.*

a. *The homomorphism of Lemma 6 is surjective.*

b. $|T(\mathfrak{P})| = e(\mathfrak{P}/\mathfrak{p})$.

c. *Let E denote the subfield of $L_{\mathfrak{P}}$ fixed by the (image of) $T(\mathfrak{P})$. Then $E/K_{\mathfrak{p}}$ is unramified of degree $f(\mathfrak{P}/\mathfrak{p})$.*

d. *$L_{\mathfrak{P}}/E$ is totally ramified of degree $e(\mathfrak{P}/\mathfrak{p})$.*

Proof. (b) implies (a): Since $T(\mathfrak{P})$ is the kernel of the homomorphism in quetion, we have

$$|\operatorname{im} G(\mathfrak{P})| = \frac{|G(\mathfrak{P})|}{|T(\mathfrak{P})|} = \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})}{e(\mathfrak{P}/\mathfrak{p})} = f(\mathfrak{P}/\mathfrak{p}) = |G(\bar{R}'/\bar{R})|.$$

Since the image and codomain have the same size, the map must be surjective.

(c) implies (b) and (d): First, we have

$$|T(\mathfrak{P})| = [L_{\mathfrak{P}} : E] = \frac{[L_{\mathfrak{P}} : K_{\mathfrak{p}}]}{[E : K_{\mathfrak{p}}]} = \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})}{f(\mathfrak{P}/\mathfrak{p})} = e(\mathfrak{P}/\mathfrak{p}),$$

which is (b). Let $\hat{\mathfrak{p}}_E$ denote the valuation ideal in E. Then what we have just proven gives

$$[L_{\mathfrak{P}} : E] = e(\mathfrak{P}/\mathfrak{p}) = e(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = e(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}_E)e(\hat{\mathfrak{p}}_E/\hat{\mathfrak{P}}) = e(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}_E),$$

the last equality coming from the fact that $E/K_{\mathfrak{p}}$ is unramified. This is the very definition of $L_{\mathfrak{P}}/E$ being totally ramified.

So we see that the rest of the theorem will follow if we can prove (c). Let $q = |\hat{R}/\hat{\mathfrak{p}}|$, $q^f = |\hat{R}'/\hat{\mathfrak{P}}|$ so that $f = f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = f(\mathfrak{P}/\mathfrak{p})$. The polynomial $x^{q^f-1} - 1$ has $q^f - 1$ distinct roots in $\hat{R}'/\hat{\mathfrak{P}}$ and Hensel's lemma then implies that these lift to distinct roots in $\hat{R}'$. In particular, one of these roots is a primitive $q^f - 1$ root of unity $\theta \in \hat{R}'$ (because one of the roots in $\hat{R}'/\hat{\mathfrak{P}}$ is a primitive $q^f - 1$ root of unity). Let $F = K_{\mathfrak{p}}(\theta)$. We have already seen that $F/K_{\mathfrak{p}}$ is unramified of degree f. If we can show that $F = E$, we will be finished. To that end, it suffices to show that F is the fixed field of (the image of) $T(\mathfrak{P})$.

We will show that an element $\sigma \in G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ fixes F if and only if $\sigma = \hat{\tau}$ for some $\tau \in T(\mathfrak{P})$. The desired result then follows from Galois theory. First of all, σ fixes F if and only if σ fixes θ. We now note that σ fixes θ if and only if $\bar{\sigma}$ fixes $\theta + \hat{\mathfrak{P}}$. The "only if" is clear. For the "if", suppose that σ *does not* fix θ. Then θ and $\sigma\theta$ are distinct roots of $x^{q^f-1} - 1$ and by our remarks above they must reduce to distinct roots in $\hat{R}'/\hat{\mathfrak{P}}$. That is, $\bar{\sigma}(\theta + \hat{\mathfrak{P}}) = \sigma\theta + \hat{\mathfrak{P}} \neq \theta + \hat{\mathfrak{P}}$, so that $\bar{\sigma}$ does not fix $\theta + \hat{\mathfrak{P}}$. Finally, being a primitive $q^f - 1$ root of unity, $\theta + \hat{\mathfrak{P}}$ generates $\hat{R}'/\hat{\mathfrak{P}}$ over $\hat{R}/\hat{\mathfrak{p}}$, and so $\bar{\sigma}$ fixes $\theta + \hat{\mathfrak{P}}$ if and only if $\bar{\sigma}$ is trivial.

We're almost done. Let σ fix F and write $\sigma = \hat{\tau}$ for some $\tau \in G(\mathfrak{P})$. We have just seen that this happens if and only if

$$1 = \bar{\sigma} = \bar{\hat{\tau}} = \hat{\bar{\tau}},$$

where we are using the notation of Lemma 8. That same lemma shows that the equation above is equivalent to $\bar{\tau} = 1$, i.e. $\tau \in T(\mathfrak{P})$. This is preciely what we needed to show. □

We continue with our usual hypotheses together with the assumption that $\mathfrak{p}$ is a finite prime of K. The chain of subgroups

$$1 \subset T(\mathfrak{P}) \subset G(\mathfrak{P}) \subset G$$

corresponds to the chain of fixed fields

$$L \supset L^{T(\mathfrak{P})} \supset L^{G(\mathfrak{P})} \supset K.$$

The field $L^{T(\mathfrak{P})}$ is called the *inertia field* of $\mathfrak{P}$ over K and $L^{G(\mathfrak{P})}$ is called the *decomposition field* of $\mathfrak{P}$ over K. As in [1], we let $\mathfrak{P}_T = \mathfrak{P} \cap L^{T(\mathfrak{P})}$, $\mathfrak{P}_Z = \mathfrak{P} \cap L^{G(\mathfrak{P})}$. Regarding these fields and ideals we prove the following result.

Theorem 9. *a. $\mathfrak{P}_T$ is the only prime of $L^{T(\mathfrak{P})}$ over $\mathfrak{P}_Z$.*

b. $\mathfrak{P}$ *is the only prime of* L *over* $\mathfrak{P}_T$.

c. We have

$$\begin{aligned} f(\mathfrak{P}/\mathfrak{p}) &= f(\mathfrak{P}_T/\mathfrak{P}_Z) = [L^{T(\mathfrak{P})} : L^{G(\mathfrak{P})}], \\ e(\mathfrak{P}/\mathfrak{p}) &= e(\mathfrak{P}/\mathfrak{P}_T) = [L : L^{T(\mathfrak{P})}], \\ e(\mathfrak{P}_T/\mathfrak{p}) &= f(\mathfrak{P}/\mathfrak{P}_T) = 1. \end{aligned}$$

Proof. This is Theorem III.1.5 of [1], and our proof is simply an elaboration on the proof given there. We start by recalling that the primes of L over $\mathfrak{P}_Z$ are permuted transitively by $G(L/L^{G(\mathfrak{P})}) = G(\mathfrak{P})$. But $\mathfrak{P}$ is such a prime, and is fixed by $G(\mathfrak{P})$. It follow that $\mathfrak{P}$ is the only prime of L over $\mathfrak{P}_Z$. This gives (a) and (b).

The basic idea behind the proof of (c) is simple: apply Theorem 8 to the Galois extension $L/L^{G(\mathfrak{P})}$. As usual though, the devil is in the details.

It is clear that the decomposition and inertia groups of $\mathfrak{P}$ in $G(L/L^{G(\mathfrak{P})}) = G(\mathfrak{P})$ are our *original* decomposition and inertia groups $G(\mathfrak{P})$ and $T(\mathfrak{P})$, respectively. Let L_T and L_Z denote the completions of the inertia and decomposition fields at the prime ideals $\mathfrak{P}_T$ and $\mathfrak{P}_Z$, respectively, viewed as subfields of $L_{\mathfrak{P}}$. In order to apply Theorem 8 we need to determine the fixed field of $T(\mathfrak{P})$ in $L_{\mathfrak{P}}$. We claim that it is L_T, as one might expect.

Given $\sigma \in G(L_{\mathfrak{P}}/L_Z) \subset G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, write $\sigma = \hat{\tau}$ for some $\tau \in G(\mathfrak{P})$. Suppose σ fixes L_T. Then $\sigma|_L = \tau$ fixes $L^{T(\mathfrak{P})}$ and so $\tau \in T(\mathfrak{P})$. Conversely, if $\tau \in T(\mathfrak{P})$ then τ fixes $L^{T(\mathfrak{P})}$, and repeating an earlier argument we find that $\hat{\tau} = \sigma$ fixes the completion L_T. This shows that, under the Galois correspondence, L_T corresponds to (the image of) $T(\mathfrak{P})$. This is what we had to show.

We have

$$[L^{T(\mathfrak{P})} : L^{G(\mathfrak{P})}] = [G(\mathfrak{P}) : T(\mathfrak{P})] = f(\mathfrak{P}/\mathfrak{p}).$$

But since $G(\mathfrak{P})$ and $T(\mathfrak{P})$ are the decomposition and inertia groups of $\mathfrak{P}$ over $L^{G(\mathfrak{P})}$, we also know that $[G(\mathfrak{P}) : T(\mathfrak{P})] = f(\mathfrak{P}/\mathfrak{P}_Z)$. The same reasoning allows us to conclude that

$$[L : L^{T(\mathfrak{P})}] = |T(\mathfrak{P})| = e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_Z).$$

Because of our work in the preceding paragraph, Theorem 8 tells us that L_T/L_Z is unramified, and hence $e(\mathfrak{P}_T/\mathfrak{P}_Z) = (\text{ramification number of } L_T/L_Z) = 1$. We also find that $L_{\mathfrak{P}}/L_T$ is totally ramified and hence $f(\mathfrak{P}/\mathfrak{P}_T) = (\text{inertial degree of } L_{\mathfrak{P}}/L_T) = 1$. Hence

$$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_Z) = f(\mathfrak{P}/\mathfrak{P}_T)f(\mathfrak{P}_T/\mathfrak{P}_Z) = f(\mathfrak{P}_T/\mathfrak{P}_Z)$$

and

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_Z) = e(\mathfrak{P}/\mathfrak{P}_T)e(\mathfrak{P}_T/\mathfrak{P}_Z) = e(\mathfrak{P}/\mathfrak{P}_T).$$

The last equation implies that $e(\mathfrak{P}_T/\mathfrak{p}) = 1$, and the proof is complete.

□

III.2

We continue with the set up of the previous section: L/K is a finite Galois extension of number fields, $\mathfrak{p}$ is a finite prime (ideal) of K and $\mathfrak{P}$ is a prime (ideal) of L extending $\mathfrak{p}$. We add the additional restriction that $\mathfrak{p}$ be unramified in L. Since L/K is Galois, this is equivalent to requiring that $e(\mathfrak{P}/\mathfrak{p}) = 1$, i.e. we only need to know "unramification" at a single prime over $\mathfrak{p}$. Recall that the *Frobenius automorphism* of $\mathfrak{P}$ is the unique element

$$\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$$

of $G(\mathfrak{P})$ satisfying

$$\sigma x \equiv x^q \pmod{\mathfrak{P}}$$

for all $x \in R' =$ algebraic integers in L, where $q = |R/\mathfrak{p}|$. It's existence and uniqueness is guaranteed by the material in section III.1 of [1].

Section III.2 established several properties of the Frobenius. We elaborate on two of them. We begin with Property III.2.2 of [1].

Theorem 10. *Let E be a field between K and L. Let $\mathfrak{p}_0 = \mathfrak{P} \cap E$. Then*

$$\left[\frac{L/K}{\mathfrak{P}}\right]^{f(\mathfrak{p}_0/\mathfrak{p})} = \left[\frac{L/E}{\mathfrak{P}}\right].$$

Proof. Since $G(L/E) \subset G(L/K)$, it is easy to see that the decomposition group $G_E(\mathfrak{P})$ of $\mathfrak{P}$ over E is contained in the decomposition group $G_K(\mathfrak{P})$ of $\mathfrak{P}$ over K. Let

$$\sigma = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Since σ has order $f(\mathfrak{P}/\mathfrak{p})$, $\tau = \sigma^{f(\mathfrak{p}_0/\mathfrak{p})}$ has order $f(\mathfrak{P}/\mathfrak{p}_0)$. Therefore τ generates the unique subgroup of $G_K(\mathfrak{P}) = \langle\sigma\rangle$ of order $f(\mathfrak{P}/\mathfrak{p}_0)$. Since $G_E(\mathfrak{P})$ is a subgroup of this order it follows that $\tau \in G_E(\mathfrak{P})$. So, to show that τ is the Frobenius of $\mathfrak{P}$ over E we now only need to show that the correct congruence is satisfied. Let $x \in R' =$ (integers of L) and let q be the size of the residue field of K. Then

$$\tau x = \sigma^{f(\mathfrak{p}_0/\mathfrak{p})} x \equiv x^{q^{f(\mathfrak{p}_0/\mathfrak{p})}} \pmod{\mathfrak{P}}.$$

This is what we needed to show since the order of the residue field of E is precisely $q^{f(\mathfrak{p}_0/\mathfrak{p})}$. □

We now make a few comments on Corollary 2.6 of [1]. This states that if E, F are two Galois extensions of K, then a prime $\mathfrak{p}$ of K splits completely in their composite $L = EF$ if and only if it splits completely in E and F. This statement is, in fact, still true if we remove the Galois assumptions, but we won't prove that here. In [1], the proof of the statement as given uses the Frobenius automorphism and is rather straighforward. However, the Frobenius only exists for unramified primes, and so the proof implicitly uses the following fact.

Lemma 9. *Let E, F be Galois extensions of K and let $L = EF$. The prime $\mathfrak{p}$ of K is unramified in L if and only it is unramified in E and F.*

Proof. The "only if" is clear. For the converse, we look at inertia groups. Let $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$ and let $\mathfrak{P}_E = \mathfrak{P} \cap E$, $\mathfrak{P}_F = \mathfrak{P} \cap F$. We need to show that $T(\mathfrak{P}) \subset G(L/K)$ is trivial. We know that restriction gives a homomorphism $G(L/K) \to G(E/K)$. We claim that this map carries $T(\mathfrak{P})$ to $T(\mathfrak{P}_E)$. First, if $\sigma \in G(\mathfrak{P})$ then $\sigma(\mathfrak{P}) = \mathfrak{P}$. Therefore $\sigma(\mathfrak{P}_E) = \sigma(\mathfrak{P} \cap E) = \mathfrak{P} \cap E = \mathfrak{P}_E$ so that $\sigma|_E \in G(\mathfrak{P}_E)$. Now let $\sigma \in T(\mathfrak{P})$. If x is any integer in E then x is an integer in L and so

$$\sigma x - x \in \mathfrak{P} \cap E = \mathfrak{P}_E.$$

Hence, $\sigma|_E \in T(\mathfrak{P}_E)$.

The rest is easy. Restriction onto each factor gives an injection

$$G(L/K) \to G(E/K) \times G(F/K)$$

that carries $T(\mathfrak{P})$ into $T(\mathfrak{P}_E) \times T(\mathfrak{P}_F)$. If $\mathfrak{P}$ were ramified over $\mathfrak{p}$ then $T(\mathfrak{P})$ would be nontrivial and this would force one of $T(\mathfrak{P}_E)$, $T(\mathfrak{P}_F)$ to be nontrivial. This would mean that $\mathfrak{p}$ ramified in either E or F, a contradiction. □

III.3

Section III.3 deals with the so-called Artin map of an *abelian* extension of number fields. Since we won't be making any explicit comments on it, we won't define it here. Of course, should the need arise, we may throw the definition in later. For now we content ourselves to provide alternate proofs of two auxiliary facts used in this section of the text.

Lemma 10. *Let L/K be a Galois extension of number fields and let E/K be an arbitrary extension of number fields. Let $\mathfrak{P}_E$ be a prime of E that is ramified in EL. Then $\mathfrak{p}_K = \mathfrak{P}_E \cap K$ is ramified in L.*

Proof. This is proved in [1] using completions. While there is nothing wrong with this approach, we provide here a proof using Galois theory and inertia groups.

Let $\mathfrak{P}_{EL}$ be a prime of EL lying over $\mathfrak{P}_E$ and let $\mathfrak{P}_L = \mathfrak{P}_{EL} \cap L$. The homomorphism $G(EL/E) \to G(L/K)$ provided by restriction is injective. An argument identical to one used earlier shows that under this map the inertia group $T(\mathfrak{P}_{EL})$ is carried into the inertia group $T(\mathfrak{P}_L)$. Since $\mathfrak{P}_E$ is ramified in EL, $T(\mathfrak{P}_{EL}) \neq 1$. It follows that $T(\mathfrak{P}_L) \neq 1$ so that $\mathfrak{p}_K$ is ramified in L. □

The end of section III.3 deals with the Artin map for cyclotomic extensions of $\mathbb{Q}$. A good deal of effort there is spent trying to determine the Frobenius of an unramified prime in a cyclotomic extension. We provide a much more elementary determination.

First the set up. Fix a positive integer $m \geq 3$ and let θ be a primitive mth root of unity. Let $L = \mathbb{Q}(\theta)$. It is well known that $L/\mathbb{Q}$ is an abelian extension of degree $\varphi(m)$ whose Galois group is isomorphic to the unit group in the ring $\mathbb{Z}/m\mathbb{Z}$. In fact, the isomorphism is provided explicitly by

$$\begin{array}{rcl} (\mathbb{Z}/m\mathbb{Z})^\times & \to & G(L/\mathbb{Q}) \\ t & \mapsto & \sigma_t \end{array}$$

where σ_t is defined by the condition

$$\sigma_t(\theta) = \theta^t.$$

Lemma 11. *Let R be the ring of integers in $L = \mathbb{Q}(\theta)$ and let p be a prime of $\mathbb{Z}$, $p \nmid m$. If $\mathfrak{p}$ is a prime of R lying over p, then $\theta + \mathfrak{p}$ is a primitive mth root of unity in $R/\mathfrak{p}$.*

Proof. We know that $\theta + \mathfrak{p}$ is an mth root of unity in $R/\mathfrak{p}$ since the same is true in R. To show that it's primitive we must show that $\theta^k \not\equiv 1 \pmod{\mathfrak{p}}$ for any $0 < k < m$. Suppose otherwise. Then there is some $0 < k < m$ so that $\theta^k \equiv 1 \pmod{\mathfrak{p}}$. Since θ is primitive, we know that $\theta^k \neq 1$. Over R the polynomial $x^m - 1$ splits as

$$x^m - 1 = \prod_{l=1}^{m}(x - \theta^l) = (x-1)(x-\theta^k) \prod_{l \neq k,m} (x - \theta^l).$$

Since $\theta^k \equiv 1 \pmod{\mathfrak{p}}$, when we reduce this polynomial mod $\mathfrak{p}$ we obtain

$$x^m - 1 \equiv (x-1)^2 \prod_{l \neq k,m} (x - \theta^l) \pmod{\mathfrak{p}}.$$

In other words, $x^m - 1$ has a repeated root in $(R/\mathfrak{p})[x]$. But $R/\mathfrak{p}$ has characteristic p, and since $p \nmid m$ we know that $x^m - 1$ is separable over $R/\mathfrak{p}$. This contradiction completes the proof. □

It is now a simple matter to determine the Frobenius of an unramified prime in L.

Proposition 4. *Let p be a prime in $\mathbb{Z}$, $p \nmid m$. Then p is unramified in $L = \mathbb{Q}(\theta)$ and its Frobenius is σ_p.*

Proof. That p is unramified in L is standard (see section I.10 of [1]). We know that there is some integer t with $(t, m) = 1$ so that the Frobenius of p is σ_t. Let $\mathfrak{p}$ be a prime of $R =$ (integers of L) lying over p. The Frobenius satisfies

$$\sigma_t x \equiv x^p \pmod{\mathfrak{p}}$$

for all $x \in R$. In particular

$$\theta^t = \sigma_t \theta \equiv \theta^p \pmod{\mathfrak{p}}.$$

The lemma tells us that $\theta + \mathfrak{p}$ is a primitive mth root of unity in $R/\mathfrak{p}$ so this congruence implies that $p \equiv t \pmod{m}$. Therefore $\sigma_t = \sigma_p$, as claimed. □

IV.1

In this section of [1] we encounter multiplicative congruences, rays, ray classes and ray class groups. Our only goal in this section of the notes is to establish some equivalences of two definitions. Let K be a number field with ring of integers R and let S be a finite set of prime ideals in R. Consider the two sets

$$\begin{aligned} K_S^1 &= \{a/b \ : \ a,b \in R, \text{ and } aR,\ bR \text{ relatively prime to all } \mathfrak{p} \in S\}, \\ K_S^2 &= \{\alpha \in K^* \ : \ \alpha R \text{ relatively prime to all } \mathfrak{p} \in S\}. \end{aligned}$$

It is clear that $K_S^1 \subset K_S^2$. In fact the two sets are identical.

Let $\alpha \in K_S^2$. Since K is the quotient field of R, we can write $\alpha = a/b$ with $a, b \in R$. Even though αR is prime to all $\mathfrak{p} \in S$, it could happen that aR or bR have prime factors in S, that just happen to cancel when we take the quotient. Our goal is to replace a and b with integers for which this is not the case.

Write $(\alpha) = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b}$ ideals in R, both relatively prime to the primes contained in S. Since the ideal class group is finite, there is an $n > 1$ so that $\mathfrak{b}^n$ is principal, $\mathfrak{b}^n = (r)$. Since $\mathfrak{b}^n \subset R$ we have $r \in R$. Also

$$(\alpha r) = (\alpha)(r) = \mathfrak{a}\mathfrak{b}^{n-1} \subset R$$

so that $\alpha r \in R$. So we have $\alpha = \alpha r / r$ with $\alpha r, r \in R$ and $(\alpha r) = \mathfrak{a}\mathfrak{b}^{n-1}$, $(r) = \mathfrak{b}^n$ are relatively prime to the ideals in S. It follows that $\alpha \in K_S^1$.

The outcome of what we've just done is the following. Given a modulus $\mathfrak{m}$ for K with finite part $\mathfrak{m}_0$, let $I_K^{\mathfrak{m}}$ denote the subgroup of the ideal group I_K generated by those primes not dividing $\mathfrak{m}_0$. Also, let $\iota : K^* \to I_K$ denote the map that carries each element of K^* to the fractional ideal it generates: $\iota(\alpha) = \alpha R$. Then the group $K_{\mathfrak{m}}$ is given by

$$\begin{aligned} K_{\mathfrak{m}} &= \{a/b \ : \ a,b \in R, \text{ and } aR,\ bR \text{ relatively prime to } \mathfrak{m}_0\} \\ &= \{\alpha \in K^* \ : \ \iota(\alpha) \in I_K^{\mathfrak{m}}\}. \end{aligned}$$

The first definition is useful if we are given an element of $K_{\mathfrak{m}}$: it tells us how we can write it down explicitly. The second definition is useful when we want to test for membership in $K_{\mathfrak{m}}$: it shows that we only need to compute the valuation of a given element at the set of primes dividing $\mathfrak{m}_0$.

We can establish a similar simplifying criterion for membership in $K_{\mathfrak{m},1}$. Indeed, we will prove that

$$\begin{aligned} K_{\mathfrak{m},1} &= \{\alpha \in K_{\mathfrak{m}} \ : \ \alpha \equiv^* 1 \pmod{\mathfrak{m}}\} \\ &= \{\alpha \in K^* \ : \ \alpha \equiv^* 1 \pmod{\mathfrak{m}}\}, \end{aligned}$$

i.e. the congruence condition automatically implies membership in $K_{\mathfrak{m}}$. To see this, let $\alpha \in K^*$ with $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$. If $\mathfrak{p}$ is a prime dividing $\mathfrak{m}_0$ with exponent $n > 0$ then $\alpha \equiv^* 1 \pmod{\mathfrak{p}^n}$ which implies that $\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(1) = 0$. It follows that $\iota(\alpha) \in I_K^{\mathfrak{m}}$, which is what we needed to show.

Let's conclude with a few (hopefully clarifying) remarks on the definition of multiplicative congruences. Let $\mathfrak{p}$ be a prime of K. If $\mathfrak{p}$ is real, corresponding to the embedding $\sigma : K \to \mathbb{R}$, let $U_{\mathfrak{p}}^{(1)} = \{\alpha \in K^* \ : \ \sigma(\alpha) > 0\}$. If $\mathfrak{p}$ is finite, corresponding to a prime ideal in R with the same name, and $n \in \mathbb{Z}^+$, let $U_{\mathfrak{p}}^{(n)} = 1 + \mathfrak{p}^n R_{\mathfrak{p}}$. In any case, $U_{\mathfrak{p}}^{(n)}$ is a subgroup of K^*, and if $\mathfrak{p}$ is finite it's moreover a subgroup of $R_{\mathfrak{p}}^{\times}$.

For $\mathfrak{p}$ a prime of K (real or finite), $n \in \mathbb{Z}^+$ ($n = 1$ if $\mathfrak{p}$ is real) and $\alpha, \beta \in K^*$, the congruence $\alpha \equiv^* \beta \pmod{\mathfrak{p}^n}$ was defined to mean that $\alpha/\beta \in U_{\mathfrak{p}}^{(n)}$, that is α and β are in the same coset of $K^*/U_{\mathfrak{p}}^{(n)}$. Given a modulus

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

we defined $\alpha \equiv^* \beta \pmod{\mathfrak{m}}$ to mean that $\alpha \equiv^* \beta \pmod{\mathfrak{p}^{n(\mathfrak{p})}}$ for all $n(\mathfrak{p}) > 0$. This collection of conditions is also equivalent to α and β lying in the same coset of K^* modulo a single subgroup. Indeed, it is easy to check that

$$K_{\mathfrak{m},1} = \bigcap_{n(\mathfrak{p})>0} U_{\mathfrak{p}}^{(n)}.$$

and that $\alpha \equiv^* \beta \pmod{\mathfrak{m}}$ if and only if α and β are in the same coset of $K^*/K_{\mathfrak{m},1}$. Thinking of multiplicative congruences in this manner can be beneficial, at least from a psychological stand point. It shows that many of the properties of the symbol $\equiv^*$ are just consequences of facts about quotient groups. It also allows us to make one final interpretation of $K_{\mathfrak{m},1}$.

We have seen that for $\alpha, \beta \in K^*$, $\alpha \equiv^* \beta \pmod{\mathfrak{m}}$ is the same thing as saying that $\alpha/\beta \in K_{\mathfrak{m},1}$. Let $\alpha \in K_{\mathfrak{m},1}$. Since $K_{\mathfrak{m},1} \subset K_{\mathfrak{m}}$ we know that there are $a, b \in R \setminus \{0\}$, both prime to $\mathfrak{m}_0$, so that $\alpha = a/b$. Since $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$, we have $a \equiv^* b \pmod{\mathfrak{m}}$. Let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{m}$ with exponent $n(\mathfrak{p}) > 0$. Because b is relatively prime to $\mathfrak{m}_0$, b is a unit in the localization $R_{\mathfrak{p}}$. Hence, $a/b - 1 \in \mathfrak{p}^{n(\mathfrak{p})}R_{\mathfrak{p}}$ if and only if $a - b \in \mathfrak{p}^{n(\mathfrak{p})}R_{\mathfrak{p}}$. That is, $a \equiv^* b \pmod{\mathfrak{p}^{n(\mathfrak{p})}}$ if and only if $a - b \in \mathfrak{p}^{n(\mathfrak{p})}R_{\mathfrak{p}} \cap R = \mathfrak{p}^{n(\mathfrak{p})}$ if and only if $a \equiv b \pmod{\mathfrak{p}^{n(\mathfrak{p})}}$. Since this is true for all the primes dividing $\mathfrak{m}_0$, we see that $a \equiv^* b \pmod{\mathfrak{m}}$ if and only if $a \equiv^* b \pmod{\mathfrak{m}_0}$ and $a \equiv^* b \pmod{\mathfrak{m}_\infty}$ if and only if $a \equiv b \mod \mathfrak{m}_0$ and $a \equiv^* b \pmod{\mathfrak{m}_\infty}$. We have therefore proven the following.

Lemma 12. *$K_{\mathfrak{m},1}$ consists of all elements of K^* of the form a/b where $a, b \in R \setminus \{0\}$ are relatively prime to $\mathfrak{m}_0$, $a \equiv b \pmod{\mathfrak{m}_0}$ and a, b have the same sign at every prime dividing $\mathfrak{m}_\infty$.*

IV.2

Dirichlet series. Let us begin by making a few remarks and clarifications on the proof of Proposition IV.2.1 of [1]. Specifically, let's look at the proof of part (c). We are given a Dirichlet series

$$f(s) = \sum_{n \geq 1} a_n n^{-s}$$

$a_n \in \mathbb{C}$, $s = \sigma + it \in \mathbb{C}$, whose summatory function

$$S(x) = \sum_{n \leq x} a_n$$

satisfies

$$\lim_{x \to \infty} \frac{S(x)}{x} = a_0.$$

The claim is that if we limit s to lie in the set $D(1, 0, \epsilon)$ for any $\epsilon > 0$ then

$$\lim_{s \to 1}(s-1)f(s) = a_0.$$

The plan is to show that this limit is equal to the analogous limit for $a_0\zeta(s)$, and then compute the latter.

The first thing to notice is that the limit condition implies $|S(x)| \leq ax$ for some $a > 0$. Thus $f(s)$ does indeed converge to a holomorphic function on $\mathrm{Re}(s) > 1$. We now apply the partial summation argument of the proof of part (a) to the partial sums of the difference $|f(s) - a_0\zeta(s)|$. This is done rather sketchily in [1], so we provide the detials. Indeed, we have

$$\begin{aligned}
\left|\sum_{n=1}^{v} a_n n^{-s} - a_0 \sum_{n=1}^{v} n^{-s}\right| &= \left|\sum_{n=1}^{v}(a_n - a_0)n^{-s}\right| \\
&= \left|(S(v) - va_0)v^{-s} + \sum_{n=1}^{v-1}(S(n) - na_0)(n^{-s} - (n+1)^{-s})\right| \\
&\leq \left|\frac{S(v)}{v} - a_0\right| v^{1-\sigma} + \sum_{n=1}^{v-1}\left|\left(\frac{S(n)}{n} - a_0\right) ns \int_n^{n+1} t^{-s-1}\, dt\right| \\
&\leq \left|\frac{S(v)}{v} - a_0\right| v^{1-\sigma} + |s| \sum_{n=1}^{\infty}\left|\frac{S(n)}{n} - a_0\right| \int_n^{n+1} t^{-\sigma}\, dt
\end{aligned}$$

Choose $M > 0$ so that $|S(x)/x - a_0| \leq M$ for all x. Let $\epsilon_0 > 0$ and choose N so that $|S(x)/x - a_0| < \epsilon_0$ for all $x \geq N$. Then the above is

$$\leq Mv^{1-\sigma} + |s|M \int_1^N t^{-\sigma}\, dt + |s|\epsilon_0 \int_N^\infty t^{-\sigma}\, dt.$$

For $\sigma > 1$ we can estimate/evaluate the integrals and let $v \to \infty$ to obtain

$$|f(s) - a_0\zeta(s)| \leq |s|MN + |s|\epsilon_0 \frac{N^{1-\sigma}}{\sigma - 1}.$$

The remainder of the argument now follows as in [1]. The main point is that as $s \to 1$, the last term on the right displays the behavior of a first order pole, so we must multiply both sides by $|s-1|$ in order to be able to take the limit as $s \to 1$. Doing so we obtain

$$|(s-1)f(s) - (s-1)a_0\zeta(s)| \leq |s-1||s|MN + |s|\epsilon_0 N^{1-\sigma} \frac{|s-1|}{\sigma - 1}.$$

It is at this point that we must enforce the restriction $s \in D(1, 0, \epsilon)$, since the rightmost term is then

$$\frac{|s-1|}{\sigma - 1} = \sec(\arg(s-1)) \leq \sec\left(\frac{\pi}{2} - \epsilon\right) = A_0.$$

Hence

$$|(s-1)f(s) - (s-1)a_0\zeta(s)| \leq |s-1||s|MN + |s|\epsilon_0 N^{1-\sigma} A_0.$$

Since $\epsilon_0 > 0$ was arbitrary it now follows that for $s \in D(1, 0, \epsilon)$

$$\lim_{s \to 1} ((s-1)f(s) - (s-1)a_0\zeta(s)) = 0.$$

One needs to exercise a little care, however, when reaching this conclusion, since N above depends on ϵ_0.

We now finish by recalling[2] the fact that $\zeta(s)$ has a pole of order 1 at $s = 1$ with residue 1. Thus

$$\lim_{s \to 1}(s-1)f(s) = \lim_{s \to 1}(s-1)a_0\zeta(s) = a_0.$$

Zeta functions. Now we turn to the zeta functions of number fields. Given a number field K, let R denote the ring of integers in K and let $\mathfrak{m}$ be a modulus for K. From now on, the symbol $\mathfrak{a}$ will always denote an *integral* ideal of K, i.e. an ideal $\mathfrak{a} \subset R$. For such an ideal $\mathfrak{a}$ we let $\mathcal{N}(\mathfrak{a}) = |R/\mathfrak{a}|$ denote the counting norm of $\mathfrak{a}$. Given a positive integer n we set

$$a_K(n) = \#\text{ ideals } \mathfrak{a},\ \mathcal{N}(\mathfrak{a}) = n$$

and given a ray class $\mathbf{k} \in I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$ we set

$$a_K(n, \mathbf{k}) = \#\text{ ideals } \mathfrak{a} \in \mathbf{k},\ \mathcal{N}(\mathfrak{a}) = n.$$

It is clear that these quantities are finite and that

$$a_K(n) = \sum_{\mathbf{k} \in I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})} a_K(n, \mathbf{k}).$$

The *zeta function of* K is defined to be

$$\zeta_K(s) = \sum_{n=1}^\infty \frac{a_K(n)}{n^s}$$

[2]For a proof, see [1] pp 144-145.

and the *zeta function of* $\mathbf{k}$ is defined to be

$$\zeta_K(s, \mathbf{k}) = \sum_{n=1}^{\infty} \frac{a_K(n, \mathbf{k})}{n^s}.$$

$\zeta_K(s, \mathbf{k})$ is sometimes referred to as a *partial zeta function*. Note that, formally at least, we have

$$\zeta_K(s, \mathbf{k}) = \sum_{\mathfrak{a} \in \mathbf{k}} \mathcal{N}(\mathfrak{a})^{-s}, \; \zeta_K(s) = \sum_{\mathfrak{a}} \mathcal{N}(\mathfrak{a})^{-s}.$$

Our main goal for now is to establish the convergence of the series defining $\zeta_K(s)$ and $\zeta_K(s, \mathbf{k})$ and prove that the formal identities above can be made meaningful. To this end, we define

$$S_K(n, \mathbf{k}) = \sum_{i=1}^{n} a_K(i, \mathbf{k}),$$

which is the summatory function of the coefficients of $\zeta_K(s, \mathbf{k})$. According to our definitions we have

$$S_K(n, \mathbf{k}) = \#\text{ ideals } \mathfrak{a} \in \mathbf{k}, \, \mathcal{N}(\mathfrak{a}) \leq n.$$

Furthermore, proposition IV.2.1 of [1] tells us that the convergence properties are related to the behavior of $S_K(n, \mathbf{k})$ as $n \to \infty$, which we now consider.

Counting Ideals in Ray Classes. What we present here essentially follows the presentation in [1], with some simplifications. Our goal is to study $S_K(n, \mathbf{k})$ by counting ideals. This we will do by reducing the problem to counting certain points in K, and then to counting lattice points in Euclidean space. We start by fixing an integral ideal $\mathfrak{c} \in \mathbf{k}^{-1}$, whose existence is guaranteed by Lemma IV.2.3 of [1]. We use this to develop our first reduction.

Lemma 13 (First Reduction). *$S_K(n, \mathbf{k})$ is the number of principal ideals (α) with $\alpha \in \mathfrak{c} \cap K_{\mathfrak{m},1}$ and $\mathcal{N}((\alpha)) \leq n\mathcal{N}(\mathfrak{c})$.*

Proof. The key observation here is that $\mathfrak{a} \in \mathbf{k}$ if and only if $\mathfrak{a}\mathfrak{c} = (\alpha)$ for some $\alpha \in \mathfrak{c} \cap K_{\mathfrak{m},1}$, which follows simply from the definition of the ray class group. That is, we have a bijection

$$\begin{array}{rcl} \{\mathfrak{a} \in \mathbf{k}\} & \longleftrightarrow & \{(\alpha) \mid \alpha \in \mathfrak{c} \cap K_{\mathfrak{m},1}\} \\ \mathfrak{a} & \longmapsto & \mathfrak{a}\mathfrak{c} = (\alpha) \\ (\alpha)\mathfrak{c}^{-1} & \longleftarrow & (\alpha). \end{array}$$

Since $\mathcal{N}$ is multiplicative, if $\mathfrak{a}$ and (α) correspond under this map, then $\mathcal{N}(\mathfrak{a}) \leq n$ if and only if $\mathcal{N}((\alpha)) \leq n\mathcal{N}(\mathfrak{c})$. □

As it stands this reduction is of only limited use, since it converts information on ideals into information on generators of principal ideals, which are not unique. While we cannot quite recover uniqueness, we can get close. We start by observing that for $\alpha, \beta \in \mathfrak{c} \cap K_{\mathfrak{m},1}$

$$(\alpha) = (\beta) \;\Leftrightarrow\; \beta = u\alpha, \; u \in U_K \cap K_{\mathfrak{m},1}$$

where $U_K = R^{\times}$ is the unit group in K. Therefore, to understand the lack of uniqueness among generators of ideals, we need to study $U_K \cap K_{\mathfrak{m},1}$.

Let $\sigma_1, \ldots, \sigma_r$ denote the real embeddings of K and let $\sigma_{r+1}, \ldots, \sigma_{r+s}$ denote the (nonconjugate) complex embeddings of K. We define two maps. The first is

$$\begin{array}{rcl} v : K & \to & \mathbb{R}^r \times \mathbb{C}^s \\ \alpha & \mapsto & (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)). \end{array}$$

To define the second let

$$\mathfrak{n} = \{(y_1, \ldots, y_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \mid y_i \neq 0 \text{ for all } i\}.$$

Then set

$$\begin{aligned} l : \mathfrak{n} &\to \mathbb{R}^{r+s} \\ (y_1, \ldots, y_{r+s}) &\mapsto (\log|y_1|, \ldots, \log|y_r|, 2\log|y_{r+1}|, \ldots, 2\log|y_{r+s}|). \end{aligned}$$

Note that v carries K^* into $\mathfrak{n}$.

These maps should be familiar to anyone who has read a proof of Dirichlet's unit theorem. Indeed, during the course of that proof it is shown that $l \circ v$ maps U_K onto an $r+s-1$ dimensional lattice consisting of vectors with coordinate sum equal to zero. Since $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ is finite, so too is $U_K/U_K \cap K_{\mathfrak{m},1}$, and we conclude that the map $l \circ v$ does the same to $U_K \cap K_{\mathfrak{m},1}$. Specifically we have the next result.

Lemma 14. *There is a finite cyclic group $\langle w \rangle$ and a free abelian group $\langle w_1, \ldots, w_{r+s-1} \rangle$ of rank $r+s-1$, both subgroups of $U_K \cap K_{\mathfrak{m},1}$, so that $U_K \cap K_{\mathfrak{m},1}$ is the internal direct product*

$$U_K \cap K_{\mathfrak{m},1} \cong \langle w \rangle \times \langle w_1, \ldots, w_{r+s-1} \rangle.$$

Moreover, the vectors $W_i = l(v(w_i))$ are linearly independent and together with the vector

$$W = (\underbrace{1, \ldots, 1}_{r}, \underbrace{2, \ldots, 2}_{s})$$

they form a basis for $\mathbb{R}^{r+s}$.

The only part of the lemma that requires some comment is the fact that W is independent of the set of W_i, which is true since the vectors W_i all have coordinate sum equal to zero. We write $\omega_{\mathfrak{m}} = |\langle w \rangle| =$ the number of roots of unity in $U_K \cap K_{\mathfrak{m},1}$. The *regulator of* $\mathfrak{m}$ is defined to be the volume of the fundamental parallelotope of the lattice $l(v(U_K \cap K_{\mathfrak{m},1}))$, which we denote by $\mathrm{reg}(\mathfrak{m})$.

Now we are in a position to pick particular representatives of our principal ideals. Given $\alpha \in K^*$, the lemma tells us that there are real numbers c, c_i so that

$$l(v(\alpha)) = cW + \sum_i c_i W_i.$$

Moreover, if $u \in U_K \cap K_{\mathfrak{m},1}$ then

$$u = w^a \prod_i w_i^{a_i}$$

for some integers a, a_i. Hence

$$l(v(u\alpha)) = l(v(u)) + l(v(\alpha)) = \left(\sum_i a_i W_i\right) + \left(cW + \sum_i c_i W_i\right) = cW + \sum_i (c_i + a_i) W_i.$$

There are unique $a_1, \ldots, a_{r+s-1} \in \mathbb{Z}$ so that $c_i + a_i \in [0,1)$. Since there are exactly $\omega_{\mathfrak{m}}$ units $u \in U_K \cap K_{\mathfrak{m},1}$ with these integers serving as exponents on the w_i (the integer a is free), we find that there are exactly $\omega_{\mathfrak{m}}$ units $u \in U_K \cap K_{\mathfrak{m},1}$ so that

$$l(v(u\alpha)) = cW + \sum_i c_i W_i, \ c \in \mathbb{R}, \ c_i \in [0,1) \text{ for all } i.$$

This gives us our next reduction.

Lemma 15 (Second Reduction). *$\omega_{\mathfrak{m}} S_K(n, \mathbf{k})$ is the number of elements $\alpha \in \mathfrak{c} \cap K_{\mathfrak{m},1}$ with $\mathcal{N}((\alpha)) \leq n\mathcal{N}(\mathfrak{c})$ and*

$$l(v(\alpha)) = cW + \sum_i c_i W_i, \ c \in \mathbb{R}, \ c_i \in [0,1) \text{ for all } i.$$

Proof. According to the arguments above, each principal ideal counted in the first reduction can be generated by exactly $\omega_{\mathfrak{m}}$ distinct elements satisfying the conditions given here. □

Getting to this reduction actually makes up the bulk of our work. For our final reduction, we need one more parameter. Since $\mathfrak{c} \in I^{\mathfrak{m}}$, we know that $\mathfrak{c}$ and $\mathfrak{m}_0$ are relatively prime ideals. Hence, by the Chinese remainder theorem, there is $\alpha_0 \in R$ so that

$$\alpha_0 \equiv 1 \pmod{\mathfrak{m}_0},\ \alpha_0 \in \mathfrak{c}.$$

Lemma 16 (Final Reduction). *$\omega_{\mathfrak{m}} S_K(n, \mathbf{k})$ is the number of $\alpha \in K^*$ so that*

a. $\alpha - \alpha_0 \in \mathfrak{m}_0\mathfrak{c}$;

b. $\alpha \equiv^* 1 \pmod{\mathfrak{m}_\infty}$;

c. $\mathcal{N}((\alpha)) \leq n\mathcal{N}(\mathfrak{c})$;

d. $l(v(\alpha)) = cW + \sum_i c_i W_i,\ c \in \mathbb{R},\ c_i \in [0,1)$ *for all* i.

Proof. It is an easy exercise to verify that for $\alpha \in R \setminus \{0\}$

$$\alpha \equiv^* 1 \pmod{\mathfrak{m}_0} \Leftrightarrow \alpha \equiv 1 \pmod{\mathfrak{m}_0}.$$

Consequently, the condition $\alpha \in \mathfrak{c} \cap K_{\mathfrak{m},1}$ in the second reduction is equivalent to the two conditions (a) and (b) above. The result follows. □

We are now in a position to count the number of α satisfying the conditions of the final reduction. Let $N : \mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}$ denote the map

$$(y_1, \ldots, y_{r+s}) \mapsto |y_1| \cdots |y_r||y_{r+1}|^2 \cdots |y_{r+s}|^2.$$

Notice that for $\alpha \in K$ we have

$$N(v(\alpha)) = |N_{K/\mathbb{Q}}(\alpha)| = \mathcal{N}((\alpha)).$$

Let Γ_0 denote the set of all $Y \in \mathbb{R}^r \times \mathbb{C}^s$ so that

i. The coordinates of Y corresponding to the real primes appearing in $\mathfrak{m}_\infty$ are positive;

ii. $0 < N(Y) \leq 1$;

iii. $l(Y) = cW + \sum_i c_i W_i,\ c \in \mathbb{R},\ c_i \in [0,1)$ for all i.

Finally, let $\mathcal{L} = v(\mathfrak{m}_0\mathfrak{c})$, $h = v(\alpha_0)$ and $\mathcal{L}_h = \mathcal{L} + h = v(\alpha_0 + \mathfrak{m}_0\mathfrak{c})$.

Lemma 17. *If $t^d = n\mathcal{N}(\mathfrak{c})$ where $d = [K : \mathbb{Q}]$ then*

$$|\mathcal{L}_h \cap t\Gamma_0| = \omega_{\mathfrak{m}} S_K(n, \mathbf{k}).$$

Proof. This really just amounts to checking the various definitions that we have made up to this point. Notice first that if $Y \in \mathbb{R}^r \times \mathbb{C}^s$ and $l(Y) = cW + \sum_i c_i W_i$, then $l(tY) = (c + \log t)W + \sum_i c_i W_i$ and $N(tY) = t^d N(Y)$. Hence, $\mathcal{L}_h \cap t\Gamma_0$ is the set of $X \in \mathbb{R}^r \times \mathbb{C}^s$ of the form $X = v(\alpha)$ for some $\alpha \in \alpha_0 + \mathfrak{m}_0\mathfrak{c}$ with positive coordinates at all the real primes dividing $\mathfrak{m}_\infty$ and satisfying $\mathcal{N}((\alpha)) = N(X) \leq t^d = n\mathcal{N}(\mathfrak{c})$, $l(v(\alpha)) = l(X) = cW + \sum_i c_i W_i,\ c \in \mathbb{R},\ c_i \in [0,1)$ for all i. That is, $\mathcal{L}_h \cap t\Gamma_0$ is the image under v of the set described in the final reduction. Since v is one-to-one, we're done. □

We now finally appeal to the following "lattice point counting" lemma, whose proof (and precise statement) may be found in [3], Chapter 6.

Lemma 18. *Let $\mathcal{L} \subset \mathbb{R}^m$ be a full lattice, $h \in \mathbb{R}^m$ and let S be a bounded subset of $\mathbb{R}^m$. If ∂S is "nice" then*

$$|\mathcal{L}_h \cap tS| = \frac{vol(S)}{vol(\mathcal{L})} t^m + O(t^{m-1})$$

for all $t > 0$. Here $vol(\mathcal{L})$ denotes the volume of a fundamental parallelotope for $\mathcal{L}$.

This lemma should seem intuitively reasonable. The volume of tS is, on the one hand, $t^m \mathrm{vol}(S)$, and, on the other hand, approximately $\mathrm{vol}(\mathcal{L})|\mathcal{L}_h \cap tS|$. The error in the approximation has to do with the parallelotopes of $\mathcal{L}_h$ that intersect the boundary of tS, which under our "nice" assumption can be thought of as being $m-1$ dimensional, and contributing $O(t^{m-1})$.

In order to apply this lemma in our situation, we need to know that the set Γ_0 is bounded and has "nice" boundary. This is proven by the methods given in [3], Chapter 6, and to save space we simply refer the reader there. We also need to know that $\mathcal{L} = v(\mathfrak{m}_0\mathfrak{c})$ is a full lattice in $\mathbb{R}^r \times \mathbb{C}^s$ (identified with $\mathbb{R}^{r+2s} = \mathbb{R}^d$). This follows from Theorem I.13.5 of [1]. Therefore, assembling the final two lemmas above we have

$$\omega_{\mathfrak{m}} S_K(n, \mathbf{k}) = \frac{\mathrm{vol}(\Gamma_0)}{\mathrm{vol}(\mathcal{L})} n\mathcal{N}(\mathfrak{c}) + O_{\mathbf{k}}(n^{1-1/d}).$$

Theorem I.13.5 of [1] also gives us that $\mathrm{vol}(\mathcal{L}) = 2^{-s}\mathcal{N}(\mathfrak{m}_0\mathfrak{c})|\Delta_K|^{1/2}$, where Δ_K is the discriminant of K. Finally, the volume of Γ_0 can be computed through straightforward means (see [1] Section II.2) to be

$$\mathrm{vol}(\Gamma_0) = 2^{r-r_0}\pi^s \mathrm{reg}(\mathfrak{m})$$

where r_0 is the number of real primes in $\mathfrak{m}_\infty$. Plugging this all in and simplifying gives us our main result.

Theorem 11.

$$\frac{S_K(n, \mathbf{k})}{n} = \frac{2^r(2\pi)^s reg(\mathfrak{m})}{\omega_{\mathfrak{m}}\mathcal{N}(\mathfrak{m})|\Delta_K|^{1/2}} + O_{\mathbf{k}}(n^{-1/d})$$

where we define $\mathcal{N}(\mathfrak{m}) = 2^{r_0}\mathcal{N}(\mathfrak{m}_0)$.

If we combine this result with Proposition IV.2.1 of [1] on Dirichlet series, we get the following statements concerning the convergence properties of the partial (and full) zeta functions of K.

Corollary 4. *The partial zeta function* $\zeta_K(s, \mathbf{k})$ *converges to a holomorphic function on* $\mathrm{Re}(s) > 1$ *and*

$$\lim_{s\to 1}(s-1)\zeta_K(s, \mathbf{k}) = g_{\mathfrak{m}} = \frac{2^r(2\pi)^s reg(\mathfrak{m})}{\omega_{\mathfrak{m}}\mathcal{N}(\mathfrak{m})|\Delta_K|^{1/2}}.$$

Moreover we can write

$$\zeta_K(s, \mathbf{k}) = \sum_{\mathfrak{a}\in\mathbf{k}} \mathcal{N}(\mathfrak{a})^{-s}$$

and the sum on the right converges absolutely for $\mathrm{Re}(s) > 1$*, uniformly for* $\mathrm{Re}(s) \geq 1+\delta$ *for any* $\delta > 0$*. In particular, the order of summation is unimportant.*

Proof. The first statement follows from the preceding theorem and Proposition IV.2.1. As for the second, notice that if $\mathrm{Re}(s) \geq 1+\delta$ then

$$|\mathcal{N}(\mathfrak{a})^{-s}| = \mathcal{N}(\mathfrak{a})^{-\sigma} \leq \mathcal{N}(\mathfrak{a})^{-1-\delta}.$$

Moreover

$$\sum_{\mathfrak{a}\in\mathbf{k}} \mathcal{N}(\mathfrak{a})^{-1-\delta} = \zeta_K(1+\delta, \mathbf{k}) < \infty$$

since the terms in the series on the left are positive, so we may rearrange them by ascending norm. It follows by the Weierstrass M-test that the series

$$\sum_{\mathfrak{a}\in\mathbf{k}} \mathcal{N}(\mathfrak{a})^{-s}$$

converges uniformly and absolutely on $\mathrm{Re}(s) \geq 1+\delta$. Consequently we can, once again, arrange the terms by ascending norm without affecting convergence to obtain

$$\zeta_K(s, \mathbf{k}) = \sum_{\mathfrak{a}\in\mathbf{k}} \mathcal{N}(\mathfrak{a})^{-s}.$$

□

Now suppose $\mathfrak{m}$ is trivial. Then $U_K \cap K_{\mathfrak{m},1} = U_K$ so that $\mathrm{reg}(\mathfrak{m}) = \mathrm{reg}(R)$ and the ray class group $I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$ is just the class group C_K. Moreover,

$$a_K(n) = \sum_{\mathbf{k} \in C_K} a_K(n, \mathbf{k})$$

and this sum is finite. This gives us our next result.

Corollary 5. *The zeta function $\zeta_K(s)$ converges to a holomorphic function on $\mathrm{Re}(s) > 1$ and*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s reg(R)}{\omega_K |\Delta_K|^{1/2}} h_K,$$

where ω_K is the number of roots of unity in K and h_K is the class number of K. Moreover

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathcal{N}(\mathfrak{a})^{-s}$$

and the sum on the right converges absolutely for $\mathrm{Re}(s) > 1$, uniformly for $\mathrm{Re}(s) \geq 1 + \delta$ for any $\delta > 0$. In particular, the order of summation is unimportant.

Proof. Take $\mathfrak{m}$ to be the trivial modulus. Then the ray class group $I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$ is just the class group C_K. Moreover,

$$a_K(n) = \sum_{\mathbf{k} \in C_K} a_K(n, \mathbf{k})$$

and this sum is finite. Hence, the convergence statements regarding the series defining $\zeta_K(s)$ follow from the analogous statements for the partial zeta functions $\zeta_K(s, \mathbf{k})$, which were proven above. In particular, notice that we have

$$\zeta_K(s) = \sum_{\mathbf{k} \in C_K} \zeta_K(s, \mathbf{k}).$$

Hence the residue of $\zeta_K(s)$ at $s = 1$ is just the sum of the residues of the $\zeta_K(s, \mathbf{k})$, which are all equal to $g_{\mathfrak{m}}$. Since $U_K \cap K_{\mathfrak{m},1} = U_K$ in this case, the formula for $g_{\mathfrak{m}}$ above gives what we want.

The second statement of the corollary is now proven exactly as above. □

Corollary 6. *$\zeta_K(s, \mathbf{k})$ (and hence $\zeta_K(s)$) can be analytically continued to the region $\mathrm{Re}(s) > 1 - 1/d$ except for a simple pole at $s = 1$.*

Proof. It is here that we make explicit use of the remainder term in Theorem 11. The coefficients of the Dirichlet series for the difference

$$\zeta_K(s, \mathbf{k}) - g_{\mathfrak{m}}\zeta(s) = \sum_{n=1}^{\infty} \frac{a_K(n, \mathbf{k}) - g_{\mathfrak{m}}}{n^s}$$

have summatory function

$$\sum_{i=1}^{n} a_K(n, s) - g_{\mathfrak{m}} = S_K(n, \mathbf{k}) - n g_{\mathfrak{m}} = O_{\mathbf{k}}(n^{1-1/d}),$$

by Theorem 11. Hence, Proposition IV.2.1 of [1] tells us that the series representing the difference converges to a holomorphic function on $\mathrm{Re}(s) > 1 - 1/d$. Since $\zeta(s)$ can be extended into this region, except for a simple pole at $s = 1$, it now follows that the same is true of $\zeta_K(s, \mathbf{k})$. □

IV.4

L-series. Here we make a few remarks on the L-series attached to a character of the ray class group. Specfically, we consider several of the convergence issues left implicit in [1], making more precise statements of some of the results proven there.

Given a number field K, a modulus $\mathfrak{m}$ for K and a character χ of the ray class group $I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$, the L-series of χ is defined to be

$$L(s,\chi) = \sum_{\mathfrak{a}\in I^{\mathfrak{m}}} \chi(\mathfrak{a})\mathcal{N}(\mathfrak{a})^{-s}.$$

Here we view χ as a character on the group $I^{\mathfrak{m}}$ by composing it with the projection of $I^{\mathfrak{m}}$ onto the ray class group. One can use the Weierstrass M-test together with Corollary 5 to see that the L-series converges absolutely for $\mathrm{Re}(s) > 1$, and uniformly for $\mathrm{Re}(s) \geq 1+\delta$, for any $\delta > 0$. In particular, we need not specify an order of summation.

Lemma 19. *For* $\mathrm{Re}(s) > 1$ *we have*

$$L(s,\chi) = \sum_{\mathbf{k}\in I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})} \chi(\mathbf{k})\zeta_K(s,\mathbf{k}).$$

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

$$\sum_{\mathbf{k}\in I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})} \chi(\mathbf{k})\zeta_K(s,\mathbf{k}) = \sum_{\mathbf{k}}\sum_{n=1}^{\infty} \chi(\mathbf{k})\frac{a_K(n,\mathbf{k})}{n^s} = \sum_{n=1}^{\infty}\left(\sum_{\mathbf{k}} \chi(\mathbf{k})a_K(n,\mathbf{k})\right)\frac{1}{n^s}.$$

The inner sum can be rewritten as

$$\sum_{\substack{\mathfrak{a}\in I^{\mathfrak{m}}\\ \mathcal{N}(\mathfrak{a})=n}} \chi(\mathfrak{a})$$

and it is therefore clear that the right-most series above is just a rearrangement of the (absolutely convergent) series defining $L(s,\chi)$. □

Notice that this lemma together with the final corollary of the preceding section tell us that $L(s,\chi)$ can be analytically continued into the region $\mathrm{Re}(s) > 1 - 1/[K:\mathbb{Q}]$, with the possible exception of a simple pole at $s = 1$. In fact, Corollary 4 together with the orthogonality relations for characters tell us that $L(s,\chi)$ is holomorphic at $s = 1$ if $\chi \neq \chi_0$ (the trivial character) while $L(s,\chi_0)$ has residue $h_{\mathfrak{m}}g_{\mathfrak{m}} > 0$ at $s = 1$. This latter fact can be viewed as the analogue of the class number formula for the order of the ray class group.

Lemma 20. *Let* $a_1,\ldots,a_r \in \mathbb{C}$, $|a_i| < 1$ *for all* i. *Then*

$$\prod_{i=1}^{r}\sum_{n=0}^{\infty} a_i^n = \sum_{(n_1,\ldots,n_r)} a_1^{n_1}\cdots a_r^{n_r}$$

where the right-hand sum is over all r*-tuples of nonnegative integers and is absolutely convergent.*

Proof. Since each geometric series on the left is absolutely convergent, a routine application of the Fubini-Tonelli theorem gives the result. □

Theorem 12 (Euler Product Representation). *For all* s *with* $\mathrm{Re}(s) > 1$ *we have*

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1}.$$

The right hand side is absolutely convergent for $\mathrm{Re}(s) > 1$ *and uniformly convergent for* $\mathrm{Re}(s) \geq 1+\delta$ *for all* $\delta > 0$.

Proof. We start by noting that

$$\left(1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1} = 1 + \frac{\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}{1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}$$

and

$$\left|\frac{\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}{1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}\right| \leq 2\mathcal{N}(\mathfrak{p})^{-\sigma}.$$

Absolute convergence of the product then follows since

$$\sum_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{-\sigma}$$

converges by Corollary 5.

Since

$$\left(1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1} = \sum_{n=1}^{\infty} \chi(\mathfrak{p}^j)\mathcal{N}(\mathfrak{p}^j)^{-s}$$

for $\mathrm{Re}(s) > 1$, we may apply the preceding lemma to conclude that for any finite set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$

$$\prod_{i=1}^{r}\left(1-\chi(\mathfrak{p}_i)\mathcal{N}(\mathfrak{p}_i)^{-s}\right)^{-1} = \sum_{(a_1,\ldots,a_r)} \frac{\chi(\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r})}{\mathcal{N}(\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r})^s}$$

the sum being over all r-tuples of nonnegative integers. Absolute convergence can then be used to show that

$$L(s,\chi) - \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m}\\ \mathcal{N}(\mathfrak{p})\leq t}} \left(1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1} = \sum_{\mathfrak{a}}{}^{*}\, \chi(\mathfrak{a})\mathcal{N}(\mathfrak{a})^{-s}$$

where the sum on the right is over all ideals $\mathfrak{a} \in I^{\mathfrak{m}}$ divisible by at least one prime $\mathfrak{p}$ with $\mathcal{N}(\mathfrak{p}) > t$. Thus, if $\mathrm{Re}(s) > 1+\delta$ then

$$\left|L(s,\chi) - \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m}\\ \mathcal{N}(\mathfrak{p})\leq t}} \left(1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1}\right| \leq \sum_{\mathcal{N}(\mathfrak{a})>t} \mathcal{N}(\mathfrak{a})^{-1-\delta}.$$

The quantity on the right is the tail of the convergent series $\zeta_K(1+\delta)$. Uniform convergence of the product to $L(s,\chi)$ follows. □

The Euler product representation allows us to conclude that $L(s,\chi)$ is zero free for $\mathrm{Re}(s) > 1$. In particular, we can define a holomorphic branch of $\log L(s,\chi)$ in this region[3]. This follows from standard results in the theory of complex variables, i.e. contour integration of the logarithmic derivative. However, we require slightly more information on the logs of L-series.

Proposition 5. *For* $\mathrm{Re}(s) > 1$

$$\log L(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s} + g_\chi(s)$$

where $g_\chi(s)$ *is holomorphic on* $\mathrm{Re}(s) > 1/2$.

Proof. If $\log z$ denotes the branch of the logarithm with imaginary part between $-\pi$ and π, it is well known that

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$$

[3]By a *holomorphic branch* of $\log f(s)$ we simply mean a holomorphic function $h(s)$ with the property that $\exp(h(s)) = f(s)$.

for $|z| < 1$. Hence, if $\mathrm{Re}(s) \geq 1 + \delta$, $\delta > 0$, then

$$\left|\log(1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})\right| \leq \sum_{n=1}^{\infty} \mathcal{N}(\mathfrak{p})^{-\sigma n} = \frac{\mathcal{N}(\mathfrak{p})^{-\sigma}}{1 - \mathcal{N}(\mathfrak{p})^{-\sigma}} \leq 2\mathcal{N}(\mathfrak{p})^{-(1+\delta)}$$

Since $\sum_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{-(1+\delta)}$ converges, the Weierstrass M-test implies that the series

$$h(s) = -\sum_{\mathfrak{p}\nmid\mathfrak{m}} \log(1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})$$

converges absolutely and uniformly to a holomorphic function on $\mathrm{Re}(s) \geq 1 + \delta$. Since $\delta > 0$ was arbitrary, we see that $h(s)$ converges absolutely to a holomorphic function on $\mathrm{Re}(s) > 1$. In particular, we have

$$\exp(h(s)) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} (1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})^{-1} = L(s, \chi)$$

for $\mathrm{Re}(s) > 1$, so that $h(s)$ gives us a branch of the logarithm of $L(s, \chi)$. Any other branch will differ from $h(s)$ by an integer multiple of $2\pi i$, and so it suffices to prove the proposition using the branch we've just defined.

The series

$$\sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}$$

converges absolutely when $\mathrm{Re}(s) > 1$. Hence, on that region we can define

$$g_\chi(s) = \log L(s, \chi) - \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \left(-\log(1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}) - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right).$$

We claim that the series on the right actually defines a holomorphic function on $\mathrm{Re}(s) > 1/2$. Using the expansion for $\log(1 - z)$ given above we see that for $\mathrm{Re}(s) \geq 1/2 + \delta$, $\delta > 0$,

$$\left|-\log(1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}) - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}\right| \leq \sum_{n=2}^{\infty} \mathcal{N}(\mathfrak{p})^{-n\sigma} = \frac{\mathcal{N}(\mathfrak{p})^{-2\sigma}}{1 - \mathcal{N}(\mathfrak{p})^{-\sigma}} \leq C\mathcal{N}(\mathfrak{p})^{-(1+2\delta)}$$

for some absolute $C > 0$. As above, the convergence of $\sum_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{-(1+2\delta)}$ and the Weierstrass M-test allow us to conclude that the series representing $g_\chi(s)$ gives a function holomorphic on $\mathrm{Re}(s) > 1/2$. □

Dirichlet Density. Given two functions $f_1(s)$ and $f_2(s)$ defined on $\mathrm{Re}(s) > 1$ we define

$$f_1 \sim f_2 \;\Leftrightarrow \lim_{s\to 1^+} f_1(s) - f_2(s) \text{ exists and is finite.}$$

We understand the limit here to mean that we approach 1 by *real* numbers $s > 1$. Note that this is restriction is not present in the definition of $\sim$ given in [1]. It is trivial to verify that $\sim$ is an equivalence relation and that is has the following property:

$$f_1 \sim f_2,\ g_1 \sim g_2,\ a \in \mathbb{C} \;\Rightarrow\; f_1 + g_1 \sim f_2 + g_2,\ af_1 \sim af_2.$$

Lemma 21. *For any fixed branch of* $\log L(s, \chi)$ *we have*

$$\log L(s, \chi) \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{-s}.$$

In particular

$$\log L(s, \chi_0) \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{-s} \sim -\log(s - 1)$$

where the right hand side is the "usual" branch of log *with imaginary part between* $-\pi$ *and* π.

Proof. The first part follows immediately from the proposition above and the definition of $\sim$. As for the second part, it suffices to prove that $\log L(s,\chi_0) \sim -\log(s-1)$. For this, choose the branch of $\log L(s,\chi_0)$ that is real on the real axis (it is clear that if the lemma holds for one branch, then it holds for them all). We know that

$$\lim_{s\to 1}(s-1)L(s,\chi_0) = h_{\mathfrak{m}} g_{\mathfrak{m}} > 0.$$

It follows that

$$\lim_{s\to 1^+} \log(s-1) + \log L(s,\chi_0) = \lim_{s\to 1^+} \log(s-1)L(s,\chi_0) = \log h_{\mathfrak{m}} g_{\mathfrak{m}},$$

which is finite. We needed to choose the particular branch of log that we did so that the identity $\log(s-1)L(s,\chi_0) = \log(s-1) + \log L(s,\chi_0)$ holds for $s > 1$. □

Let S be a set of prime ideals in our number field K. If there is a real number δ so that

$$-\delta \log(s-1) \sim \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s}$$

then we say that S has *Dirichlet density* δ and we write $\delta(S) = \delta$. It is not true that every set S possesses a Dirichlet density (although we won't give an example a set without). Therefore, any time we write $\delta(S) = \cdots$ we will mean "S has Dirichlet density and it is equal to $\cdots$".

As a first example consider the set S of all prime ideals in K. If we let $\mathfrak{m}$ denote the trivial modulus in Lemma 21, we see immediately that $\delta(S) = 1$ (again, this means S has Dirichlet density and it is equal to 1). A little more generally, if S' is a finite set of prime ideals and $\mathfrak{m} = \prod_{\mathfrak{p}\in S'} \mathfrak{p}$, then the same lemma tells us that $\delta(S \setminus S') = 1$. Before turning to some more complicated examples, we first state and prove some useful properties of the Dirichlet density.

Theorem 13 (Properties of Dirichlet Density). *Let S, S' and T denote sets of prime ideals of K.*

1. *If S is finite then $\delta(S) = 0$.*
2. *If $S \subset S'$ and $\delta(S), \delta(S')$ both exist then $\delta(S) \le \delta(S')$.*
3. *If $\delta(S)$ exists then $\delta(S) \in [0,1]$.*
4. *If $S \subset S'$ and $\delta(S') = 0$ then $\delta(S) = 0$.*
5. *If $\delta(S)$ exists and $\delta(S') = 0$ then $\delta(S \setminus S') = \delta(S) = \delta(S \cup S')$.*
6. *If $S \subset T \subset S'$ and $\delta(S), \delta(S')$ exist and are equal, then $\delta(S) = \delta(T) = \delta(S')$.*

Proof. If S is finite then

$$\lim_{s\to 1^+} \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s}$$

exists and is finite. Hence it is $\sim -0\log(s-1)$ and $\delta(S) = 0$.

If $S \subset S'$ then we have

$$-\delta(S')\log(s-1) \sim \sum_{\mathfrak{p}\in S'} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s} \sim -\delta(S)\log(s-1) + \sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s}$$

or

$$\sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s} \sim -(\delta(S') - \delta(S))\log(s-1)$$

Since $\sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s}$ is nonnegative and increasing for $s \to 1^+$, and $\log(s-1) \to -\infty$ as $s \to 1^+$, this is only possible if $\delta(S') - \delta(S) \ge 0$

If $\delta(S)$ exists then, taking S' to be the set of all primes, we have $S \subset S'$ so that, by what we have just shown, $\delta(S) \le \delta(S') = 1$. Also, since

$$-\delta(S)\log(s-1) \sim \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s}$$

and the right hand side is nonnegative and increasing as $s \to 1^+$, we may argue as above that $\delta(S) \geq 0$.

Now suppose $S \subset S'$ and $\delta(S') = 0$. Then, since all of the functions involved are increasing as $s \to 1^+$ (so that existence of the limits is guaranteed) we have

$$\lim_{s\to 1^+} \sum_{\mathfrak{p}\in S'} \mathcal{N}(\mathfrak{p})^{-s} = \lim_{s\to 1^+} \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} + \lim_{s\to 1^+} \sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s}.$$

Since $\delta(S') = 0$, the limit on the left is finite. Since the limits on the right are both nonnegative, both must be finite as well. Hence, $\delta(S) = \delta(S' \setminus S) = 0$.

If $\delta(S)$ exists and $\delta(S') = 0$ then, according to what we have just done, $\delta(S \cap S') = \delta(S' \setminus S) = 0$. Thus

$$-\delta(S)\log(s-1) \sim \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\in S\setminus S'} \mathcal{N}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}\in S\cap S'} \mathcal{N}(\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}\in S\setminus S'} \mathcal{N}(\mathfrak{p})^{-s}$$

and

$$-\delta(S)\log(s-1) \sim \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\in S\cup S'} \mathcal{N}(\mathfrak{p})^{-s} - \sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}\in S\cup S'} \mathcal{N}(\mathfrak{p})^{-s}$$

which give the desired conclusion.

Finally, if $S \subset T \subset S'$ and $\delta(S) = \delta(S')$ then

$$0 = -(\delta(S') - \delta(S))\log(s-1) \sim \sum_{\mathfrak{p}\in S'} \mathcal{N}(\mathfrak{p})^{-s} - \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\in S'\setminus S} \mathcal{N}(\mathfrak{p})^{-s}$$

so that $\delta(S' \setminus S) = 0$. Since $T \setminus S \subset S' \setminus S$ it follows from above that $\delta(T \setminus S) = 0$. Since $T = S \cup (T \setminus S)$, we're done by the previous paragraph. □

A few comments on these properties are in order. It is typical to use Property 1 in the form of its converse: if $\delta(S) > 0$ then S is infinite. Property 5 tells us that we may alter a set S by a set of density zero without affecting the original density of S. In particular, if we add to or remove from S a set of density zero, and then show the density of the new set S' exists, we can conclude that the density of S exists an equals that of S'. If we apply Property 6 with $\delta(S) = 1$ and S' the set of all primes, then we get the following useful statement: if $S \subset T$ and $\delta(S) = 1$, then $\delta(T) = 1$.

We now compute the densities of some nontrivial sets of primes.

Theorem 14. *Let S denote the set of prime ideals $\mathfrak{p}$ of K with $f(\mathfrak{p}|\mathfrak{p}\cap\mathbb{Q}) = 1$. Then $\delta(S) = 1$.*

Proof. Let S' be the complementary set of primes. Then

$$-\log(s-1) \sim \sum_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\in S} \mathcal{N}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}\in S'} \mathcal{N}(\mathfrak{p})^{-s}$$

so it suffices to show that $\delta(S') = 0$.

Given a prime $\mathfrak{p} \in S'$ we have $\mathcal{N}(\mathfrak{p}) \geq p^2$ where $(p) = \mathfrak{p}\cap\mathbb{Q}$. Hence, for $s > 1$

$$\sum_{\mathfrak{p}\in S'} \mathcal{N}(\mathfrak{p})^{-s} = \sum_{p} \sum_{\substack{\mathfrak{p}\in S' \\ \mathfrak{p}|p}} \mathcal{N}(\mathfrak{p})^{-s} \leq [K:\mathbb{Q}] \sum_{p} p^{-2s} \leq [K:\mathbb{Q}]\zeta(2).$$

Since the sum on the left is increasing as $s \to 1^+$, this allows us to conclude that it's limit at 1^+ is finite. So $\delta(S') = 0$. □

Corollary 7. *Let L/K be number fields, $S = \{\mathfrak{P} \subset R_L \mid f(\mathfrak{P}|\mathfrak{P}\cap K) = 1\}$. Then $\delta(S) = 1$.*

Proof. Since inertial degrees are multiplicative

$$S \supset S' = \{\mathfrak{P} \subset R_L \mid f(\mathfrak{P}|\mathfrak{P}\cap\mathbb{Q}) = 1\}.$$

Hence $1 = \delta(S') = \delta(S)$. □

Theorem 15. *Let L/K be a Galois extension of number fields and let S denote the set of prime ideals of K that split completely in L. Then*

$$\delta(S) = \frac{1}{[L:K]}.$$

Proof. Let S_L denote the set of all primes of L that lie over primes of S. If $\mathfrak{p} \in S_1$ then $\mathfrak{p}$ has $[L:K]$ divisors in S_L and for any such $\mathfrak{P}$ we have $\mathcal{N}(\mathfrak{P}) = \mathcal{N}(\mathfrak{p})$ since splitting completely forces $f(\mathfrak{P}|\mathfrak{p}) = 1$. Thus

$$\sum_{\mathfrak{P}\in S_L} = \mathcal{N}(\mathfrak{P})^{-s} = \sum_{\mathfrak{p}\in S}\sum_{\mathfrak{P}|\mathfrak{p}} \mathcal{N}(\mathfrak{P})^{-s} = [L:K]\sum_{\mathfrak{p}\in S}\mathcal{N}(\mathfrak{p})^{-s}.$$

So we will be finished if we can show that $\delta(S_L) = 1$. But this is easy: let S^* denote the set of primes $\mathfrak{P}$ of L for which $f(\mathfrak{P}|\mathfrak{P}\cap K) = 1$. Since there are only finitely many of them, we may remove the primes of S^* that lie over ramified primes in K without changing the density. The Galois assumption then implies that $S^* \subset S_L$. Since $\delta(S^*) = 1$ by the previous theorem, we conclude that $\delta(S_L) = 1$ as well, proving the theorem. □

A nice corollary to this result is the following.

Corollary 8. *Let L_1, L_2 be finite Galois extensions of the number field K and let S_i be the set of primes of K that split completely in L_i ($i = 1, 2$). Then $S_1 \subset S_2$ (except on a set of density zero) if and only if $L_2 \subset L_1$*

Proof. If $L_2 \subset L_1$ then it is clear that $S_1 \subset S_2$. So we need only prove the converse. Let $L = L_1L_2$. We know that L/K is Galois and that $\mathfrak{p}$ splits completely in L if and only if $\mathfrak{p} \in S_1 \cap S_2$. The theorem and our hypothesis that $S_1 \subset S_2$ except on a set of density zero then give

$$[L:K]^{-1} = \delta(S_1 \cap S_2) = \delta(S_1) = [L_1:K]^{-1}.$$

From this we conclude that $L_1 = L = L_1L_2 \supset L_2$. □

Theorem 16. *Let K be a number field and let $\mathfrak{m}$ be a modulus for K. Let H be a group satisfying $\iota(K_{\mathfrak{m},1}) \subset H \subset I^{\mathfrak{m}}$ and set $h = [I^{\mathfrak{m}} : H]$. Let S be a set of prime ideals in K with $S \subset H$. If $\delta(S)$ exists then*

$$\delta(S) \leq \frac{1}{h}$$

Proof. Let χ be a character on $I^{\mathfrak{m}}/H$. Via the composition

$$I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1}) \to I^{\mathfrak{m}}/H \to \mathbb{C}^*$$

we may view χ as a character of the ray class group. For a prime $\mathfrak{p}$ of K the orthogonality relations give

$$\sum_{\chi\in\widehat{I^{\mathfrak{m}}/H}} \chi(\mathfrak{p}) = \begin{cases} 0, & \mathfrak{p} \notin H \\ h, & \mathfrak{p} \in H \end{cases}$$

Hence

$$\sum_{\chi}\log L(s,\chi) \sim \sum_{\chi}\sum_{\mathfrak{p}\nmid\mathfrak{m}}\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}\nmid\mathfrak{m}}\left(\sum_{\chi}\chi(\mathfrak{p})\right)\mathcal{N}(\mathfrak{p})^{-s} = h\sum_{\mathfrak{p}\in H}\mathcal{N}(\mathfrak{p})^{-s}.$$

Also

$$\sum_{\chi}\log L(s,\chi) \sim -\log(s-1) + \sum_{\chi\neq\chi_0}\log L(s,\chi).$$

Putting these together we find

$$\sum_{\mathfrak{p}\in H}\mathcal{N}(\mathfrak{p})^{-s} \sim -\frac{1}{h}\log(s-1) + \frac{1}{h}\sum_{\chi\neq\chi_0}\log L(s,\chi). \tag{3}$$

If S has density $\delta(S)$ then

$$-\delta(S)\log(s-1) \sim \sum_{\mathfrak{p}\in S}\mathcal{N}(\mathfrak{p})^{-s} \sim -\frac{1}{h}\log(s-1) + \frac{1}{h}\sum_{\chi\neq\chi_0}\log L(s,\chi) - \sum_{\mathfrak{p}\in H\setminus S}\mathcal{N}(\mathfrak{p})^{-s}.$$

That is

$$\lim_{s\to 1^+}\left(\left(\delta(S)-\frac{1}{h}\right)\log(s-1) + \frac{1}{h}\sum_{\chi\neq\chi_0}\log L(s,\chi) - \sum_{\mathfrak{p}\in H\setminus S}\mathcal{N}(\mathfrak{p})^{-s}\right)$$

exists and is finite. Consider the two right hand terms. As $s\to 1^+$: the final term decreases; if $L(1,\chi)\neq 0$ then $\log L(s,\chi)\to\log L(1,\chi)$; if $L(1,\chi)=0$ then $\log|L(s,\chi)|\to-\infty$. Consequently, the only way the limit can be finite is if $\delta(S)-1/h\leq 0$, which is what we sought to show. □

If we put equation (3) together with the reasoning just given concerning $\log L(s,\chi)$ as $s\to 1^+$ we immediately deduce the next result.

Proposition 6. *Given the set up of the previous theorem, if S is the set of all primes in H then $\delta(S)=1/h$ if and only if $L(1,\chi)\neq 0$ for all nontrivial characters χ of the group $I^{\mathfrak{m}}/H$.*

IV.5

As in [1], given a group G and an element $\sigma\in G$ of order n, we define the *division* of σ to be the set

$$\{\tau\sigma^m\tau^{-1} \mid \tau\in G,\ (m,n)=1\}.$$

This is the set of all conjugates of generators of the cyclic group $\langle\sigma\rangle$. We let t denote the number of elements in the division of σ. It is proven in [1] (Proposition IV.5.1) that if G is finite and $H=\langle\sigma\rangle$ then

$$t=\phi(n)[G:N_G(H)]$$

where ϕ is Euler's phi function.

Our goal here is to simplify the exposition in [1] of the Frobenius density theorem and its consequences through the next lemma.

Lemma 22. *Let L/K be a Galois extension of number fields and let $\sigma\in G(L/K)$. Set*

$$S=\left\{\mathfrak{p}\subset R_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and there is a } \mathfrak{P}\subset R_L \text{ with } \mathfrak{P}|\mathfrak{p} \text{ and } \left[\frac{L/K}{\mathfrak{P}}\right] \text{ in the division of } \sigma\right\}$$

and

$$S'=\left\{\mathfrak{p}\subset R_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and there is a } \mathfrak{P}\subset R_L \text{ with } \mathfrak{P}|\mathfrak{p} \text{ and } \left[\frac{L/K}{\mathfrak{P}}\right] \text{ generating } \langle\sigma\rangle\right\}.$$

Then $S=S'$.

Proof. Let $\mathfrak{p}\in S$ and choose $\mathfrak{P}$ over $\mathfrak{p}$ with $\left[\frac{L/K}{\mathfrak{P}}\right]$ in the division of σ. Then

$$\left[\frac{L/K}{\tau\mathfrak{P}}\right]=\tau\left[\frac{L/K}{\mathfrak{P}}\right]\tau^{-1}=\sigma^m$$

for some $\tau\in G(L/K)$ and $(m,n)=1$, where n is the order of σ. Replacing $\mathfrak{P}$ by $\tau\mathfrak{P}$ we see that $\mathfrak{p}\in S'$ since σ^m generates $\langle\sigma\rangle$.

Conversely, if $\mathfrak{p}\in S'$ then there is a $\mathfrak{P}$ over $\mathfrak{p}$ so that

$$\left[\frac{L/K}{\mathfrak{P}}\right]=\sigma^m$$

where $(m,n)=1$, n being the order of σ, since the generators of $\langle\sigma\rangle$ all have this form. Hence, $\left[\frac{L/K}{\mathfrak{P}}\right]$ is in the division of σ and $\mathfrak{p}\in S$. □

We point out that the condition that $\left[\frac{L/K}{\mathfrak{P}}\right]$ generate $\langle\sigma\rangle$ is equivalent to saying that $G(\mathfrak{P}) = \langle\sigma\rangle$. The lemma tells us that the formulation of the Frobenius density theorem we give below is equivalent to that given in [1].

Theorem 17 (Frobenius Density Theorem). *Let L/K be a Galois extension of number fields and let $\sigma \in G(L/K) = G$ have order n, with t elements in its division. Set*

$$S_1 = \left\{\mathfrak{p} \subset R_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and there is a } \mathfrak{P} \subset R_L \text{ with } \mathfrak{P}|\mathfrak{p} \text{ and } \left[\frac{L/K}{\mathfrak{P}}\right] \text{ generating } \langle\sigma\rangle\right\}.$$

Then

$$\delta(S_1) = \frac{t}{|G|}.$$

Proof. We induct on n. When $n = 1$, $\sigma = 1$ and so S_1 is just the set of primes in K that split completely in L. We have already seen that this set has density

$$\delta(S_1) = \frac{1}{[L:K]} = \frac{1}{|G|}.$$

This proves the theorem when $n = 1$.

Now let $n > 1$ and assume that the theorem has been proven for all elements of G with order $< n$. For $d|n$ let

$$\begin{aligned} t_d &= \text{number of elements in the division of } \sigma^d \\ S_d &= \left\{\mathfrak{p} \subset R_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and there is a } \mathfrak{P} \subset R_L \text{ with } \mathfrak{P}|\mathfrak{p} \text{ and } \left[\frac{L/K}{\mathfrak{P}}\right] \text{ generating } \langle\sigma^d\rangle\right\}. \end{aligned}$$

The inductive hypothesis implies that $\delta(S_d) = t_d/|G|$ for $d \neq 1$.

Let $H = \langle\sigma\rangle$ and let $E = L^H$. Let S_E denote the set of primes P of E with $f(P|P \cap K) = 1$. We claim that a prime $\mathfrak{p}$ of K unramified in L is divisible by a prime $P \in S_E$ if and only if $\mathfrak{p} \in S_d$ for some $d|n$. Let $\mathfrak{p}$ be a prime K unramified in L and fix a prime $\mathfrak{Q}$ of L over $\mathfrak{p}$. If we appeal to Corollary III.2.8 of [1], we see that there is a prime $P \in S_E$ over $\mathfrak{p}$ if and only if there is a $\tau \in G$ so that $\tau G(\mathfrak{Q})\tau^{-1} \subset H$. Since $\tau G(\mathfrak{Q})\tau^{-s} = G(\tau\mathfrak{Q})$ and G transitively permutes the primes of Lover $\mathfrak{p}$, we see that this last condition is equivalent to the statement that $\mathfrak{p}$ is divisible by a prime $\mathfrak{P}$ of L with $G(\mathfrak{P}) \subset H$. But H is cyclic and generated by σ. Thus, $G(\mathfrak{P}) \subset H$ if and only if $G(\mathfrak{P}) = \langle\sigma^d\rangle$ for some $d|n$. This is equivalent to saying that $\mathfrak{p} \in S_d$ for some $d|n$.

For $\mathfrak{p} \in S_d$ we define $n(\mathfrak{p})$ to be the number of $P \in S_E$ dividing $\mathfrak{p}$. Notice that if P is such a prime then $f(P|\mathfrak{p}) = 1$ so that $\mathcal{N}(P) = \mathcal{N}(\mathfrak{p})$. Since S_E has Dirichlet density 1 we therefore have

$$-\log(s-1) \sim \sum_{P \in S_E} \mathcal{N}(P)^{-s} \sim \sum_{d|n} \sum_{\mathfrak{p} \in S_d} \sum_{\substack{P|\mathfrak{p} \\ P \in S_E}} \mathcal{N}(P)^{-s} = \sum_{d|n} \sum_{\mathfrak{p} \in S_d} n(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}.$$

The second "$\sim$" comes from the fact that we must discard from S_E the (finite number of) primes P for which $P \cap K$ is ramified in L. To finish the proof we will compute the numbers $n(\mathfrak{p})$, showing that they are constant for each value of d.

So fix $\mathfrak{p} \in S_d$ for some $d|n$. Choose a prime $\mathfrak{P}$ of L over $\mathfrak{p}$ with $G(\mathfrak{P}) = \langle\sigma^d\rangle$. Again appealing to Corollary III.2.8 of [1], we find that $n(\mathfrak{p})$ is the number of cosets $H\gamma$ so that $\gamma G(\mathfrak{P})\gamma^{-1} \subset H$. Since H is generated by σ, it has a unique subgroup of any given order. Thus, $\gamma G(\mathfrak{P})\gamma^{-1} \subset H$ is equivalent to $\gamma\langle\sigma^d\rangle\gamma^{-1} = \langle\sigma^d\rangle$, which in turn is equivalent to $\gamma \in N_G(\langle\sigma^d\rangle)$. It follows that

$$n(\mathfrak{p}) = [N_G(\langle\sigma^d\rangle) : H] \text{ for } \sigma \in S_d.$$

We substitute this result into the above and use the fact that $\delta(S_d) = t_d/|G|$ for $d \neq 1$. We obtain

$$\begin{aligned} -\log(s-1) &\sim \sum_{d|n} [N_G(\langle\sigma^d\rangle) : H] \sum_{\mathfrak{p} \in S_d} \mathcal{N}(\mathfrak{p})^{-s} \\ &\sim -\left(\sum_{\substack{d|n \\ d \neq 1}} \frac{[N_G(\langle\sigma^d\rangle) : H]t_d}{|G|}\right) \log(s-1) + [N_G(H) : H] \sum_{\mathfrak{p} \in S_1} \mathcal{N}(\mathfrak{p})^{-s}. \end{aligned}$$

Since $t_d = \phi(n/d)[G : N_G(\langle\sigma^d\rangle)]$ and $t = \phi(n)[G : N_G(H)]$ this can be rearranged as

$$\sum_{\mathfrak{p}\in S_1} \mathcal{N}(\mathfrak{p})^{-s} \sim \left(-1 + \frac{1}{n}\sum_{\substack{d|n\\ d\neq 1}} \phi(n/d)\right) \frac{nt}{\phi(n)|G|} \log(s-1).$$

The conclusion finally follows from the well known identity

$$\sum_{d|n} \phi(d) = n.$$

□

We now quickly deduce some consequences of the Frobenius density theorem in the case that L/K is abelian.

Corollary 9. *Let L/K be an abelian extension of number fields, $\sigma \in G(L/K) = G$ with order n. If*

$$S = \{\mathfrak{p} \subset R_K \mid (L/K, \mathfrak{p}) \text{ generates } \langle\sigma\rangle\}$$

then

$$\delta(S) = \frac{\phi(n)}{|G|}.$$

Proof. We simply notice that since G is abelian the division of σ consists only of the generators of $\langle\sigma\rangle$, of which there are $\phi(n)$. The conclusion follows at once from the Frobenius density theorem. □

Corollary 10 (Surjectivity of the Artin Map). *Let L/K be an abelian extension of number fields. Let S be a finite set of primes in K including all of those that ramify in L. Then $\varphi_{L/K} : I_K^S \to G(L/K)$ is surjective.*

Proof. Let $\sigma \in G$. The first corollary gives us infinitely many $\mathfrak{p}$ of K so that $(L/K, \mathfrak{p})$ generates $\langle\sigma\rangle$. In particular, we can find such a prime $\mathfrak{p} \in I_K^S$. Then $\varphi_{L/K}(\mathfrak{p}) = (L/K, \mathfrak{p})$ generates $\langle\sigma\rangle$ so that $\sigma \in \varphi_{L/K}(I_K^S)$. □

Corollary 11. *Let L/K be a cyclic extension of number fields of degree n with group generated by σ. For $d|n$ let S_d denote the set of primes in K that have exactly d prime divisors in L. Then $\delta(S_d) = \phi(n/d)/n$.*

Proof. After discarding from S_d the finite number of primes that ramify in L (which has no impact on the density) we see that $\mathfrak{p} \in S_d$ if and only if $(L/K, \mathfrak{p})$ has order n/d if and only if $(L/K, \mathfrak{p})$ generates $\langle\sigma^d\rangle$ (since $G(L/K)$ is generated by σ). The set of unramified primes with this final property has density $\phi(n/d)/n$ by the first corollary. □

Primes in Progressions. Although we didn't cover it in class, the Frobenius Density Theorem can be used to prove Dirichlet's theorem on primes in progressions. We refer the reader, as usual, to [1] for most of the argument, and provide here only a few of the details.

Let be m a positive integer, ω a primitive mth root of unity and $L = Q(\omega)$. We let S denote the set of all primes in $\mathbb{Z}$ dividing m. Proposition III.3.1 of [1] shows that the Artin map $\varphi_{L/\mathbb{Q}} : I^S \to G(L/\mathbb{Q})$ is surjective with kernel consisting of all fractional ideals of the form (a/b) where a, b are positive integers relatively prime to m satisfying $a \equiv b \pmod m$. Let $\mathfrak{m}$ be the modulus $p_\infty(m)$ for $\mathbb{Q}$. Then $I^S = I^{\mathfrak{m}}$ and Lemma 12 above shows that the kernel of $\varphi_{L/\mathbb{Q}}$ is precisely $\iota(\mathbb{Q}_{\mathfrak{m},1})$. That is, the Artin map furnishes an isomorphism of the ray class group $I^{\mathfrak{m}}/\iota(\mathbb{Q}_{\mathfrak{m},1})$ with the Galois group $G(L/\mathbb{Q})$. It follows immediately that $h_{\mathfrak{m}} = [I^{\mathfrak{m}} : \iota(\mathbb{Q}_{\mathfrak{m},1})] = \phi(m)$.

Continuing with the set up of the previous paragraph, let χ be a Dirichlet character mod m. In view of the isomorphism we've just described and the isomorphism $G(L/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ we may view χ as a character on the ray class group $I^{\mathfrak{m}}/\iota(\mathbb{Q}_{\mathfrak{m},1})$. Thus, we can attach two Dirichlet series to χ: a classical

Dirichlet L-function as well as the L-series of a ray class group character. Not surprisingly, these objects turn out to be the same!

To see this, let $\tilde{\chi}$ denote the character χ gives on the ray class group. The Dirichlet L-function can be written as an Euler product over the primes p of $\mathbb{Z}$ not dividing m. The L-series of $\tilde{\chi}$ can also be written as an Euler product, this time over the prime ideals of $\mathbb{Z}$ not dividing $\mathfrak{m}$. It is clear that these two sets of primes coincide. Thus, we need only show that for a given $p \nmid m$, the two corresponding factors in the Euler products of $L(s,\chi)$ and $L(s,\tilde{\chi})$ agree.

The factor in $L(s,\chi)$ corresponding to p is $(1-\chi(p)p^{-s})^{-1}$. The factor in $L(s,\tilde{\chi})$ is $(1-\tilde{\chi}((p))\mathcal{N}((p))^{-s})^{-1}$. We know $\mathcal{N}((p)) = p$, so we only need to show that $\chi(p) = \tilde{\chi}((p))$. We have seen that the Artin map carries (p) to the automorphism σ_p (which maps ω to ω^p). The isomorphism of $G(L/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^*$ identifies σ_p with the class of p mod m and so, by the definition of $\tilde{\chi}$, we have $\tilde{\chi}((p)) = \chi(\text{image of } (p) \text{ in } (\mathbb{Z}/m\mathbb{Z})^*) = \chi(p)$.

The primes of $\mathbb{Q}$ that are unramified in L with trivial Frobenius have Dirichlet density $[L:\mathbb{Q}]^{-1} = \phi(m)^{-1}$, by the Frobenius density theorem. At the same time, we have seen that these are, with finitely many exceptions, precisely the primes in the kernel of the Artin map, which is $\iota(\mathbb{Q}_{\mathfrak{m},1})$. Hence, the primes of $\mathbb{Q}$ in $\iota(\mathbb{Q}_{\mathfrak{m},1})$ have density $\phi(m)^{-1} = [I^{\mathfrak{m}} : \iota(\mathbb{Q}_{\mathfrak{m},1})]^{-1}$. It follows from Proposition 6 that the L-series attached to a nontrivial character χ of the ray class group $I^{\mathfrak{m}} : \iota(\mathbb{Q}_{\mathfrak{m},1})$ does not vanish at $s = 1$. Our argument above now allows us to recover the following classical result.

Theorem 18. *If χ is a nontrivial Dirichlet character mod m then $L(1,\chi) \neq 0$.*

This is a crucial ingredient in Dirichlet's original proof of his theorem on primes in arithmetic progressions. In fact, the proof given in [1] is just a translation of this proof into the language of class field theory.

V.1

Here we add a few basic facts to the collection of cohomological information contained in the corresponding section of [1]. For the basic definitions of cohomology (of finite cyclic groups) and Herbrand quotients, see [1]. Let me begin by recalling the following fundamental lemma, which is a consequence of the so-called Exact Hexagon Lemma (see [1]).

Lemma 23. *Let G be a finite cyclic group and A, B, C be G-modules. If there is an exact sequence*

$$0 \to A \to B \to C \to 0$$

of G-modules and any two of $q(A)$, $q(B)$, $q(C)$ are defined, then so is the third and

$$q(A)q(C) = q(B)$$

One consequence of this fact is the following.

Lemma 24. *Let A_i be a G-module for $i = 1, \ldots, n$ and let*

$$A = \bigoplus_{i=1}^{n} A_i$$

be a G-module via the diagonal action. If $q(A_i)$ is defined for all i then so is $q(A)$ and

$$q(A) = \prod_{i=1}^{n} q(A_i).$$

Proof. When $n = 2$ we have the exact sequence of G-modules

$$0 \to A_1 \to A_1 \oplus A_2 \to A_2 \to 0$$

which proves the result in this case, is view of the preceding lemma. Induction yields the general result. □

The next result, while surely expected, deserves proof nonetheless.

Corollary 12. *If A and B are isomorphic G-modules and one of $q(A), q(B)$ is defined then they both are and*

$$q(A) = q(B).$$

Proof. There is an exact sequence

$$0 \to A \to B \to 0 \to 0.$$

Now use the first lemma and the fact that $q(C) = 1$ for any finite G-module C. □

V.2

Maps on Ideals. Let L/K be an extension of number fields. We recall two fundamental homomorphisms that allow us to pass between the groups I_K and I_L,

The *norm* homomorphism $N_{L/K} : I_L \to I_K$ is defined on prime ideals $\mathfrak{P}$ of L by

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$$

where $\mathfrak{p} = \mathfrak{P} \cap K$ and $f = f(\mathfrak{P}|\mathfrak{p})$. Since I_L is free on the set of prime ideals $\mathfrak{P}$, this equation uniquely defines $N_{L/K}$ on all of I_L. If E is a field between L/K then it is easy to use the multiplicativity of inertial degrees to show that we have $N_{E/K} \circ N_{L/E} = N_{L/K}$ for the composite map.

Although we won't have any use for it, we point out another interesting interpretation of the the norm map which perhaps lends more credence to its name. Given a fractional ideal $\mathfrak{A}$ of L let $\mathfrak{a}$ denote the fractional ideal of K generated by all elements of the form $N_{L/K}(a)$ for $a \in \mathfrak{A}$. Then it turns out that

$$N_{L/K}(\mathfrak{A}) = \mathfrak{a}.$$

In fact, if one defines the norm map through this equation, then this definition is equivalent to the one that we have given. See [4] for half of the equality, [1] for the other. Which formula one chooses as the definition of $N_{L/K}$ depends (as far as I can tell) only on whether or not one wishes to deduce properties of the discriminant ideal $\Delta(L/K)$ from $N_{L/K}$ or vice-versa.

The *injection* homomorphism $i_{L/K} : I_K \to I_L$ is given for a fractional ideal $\mathfrak{a} \in I_K$ by

$$i_{L/K}(\mathfrak{a}) = \mathfrak{a}R_L.$$

If $\mathfrak{p}$ is a prime ideal of K and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are the primes of L over $\mathfrak{p}$ with ramification numbers $e_1, \ldots, e_g$ respectively then

$$i_{L/K}(\mathfrak{p}) = \mathfrak{p}R_L = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_g^{e_g}. \tag{4}$$

In fact, since I_K is freely generated by such $\mathfrak{p}$ one can, as above, use this to define $i_{L/K}$ in a purely algebraic fashion.

Proposition 7. *Let L/K be number fields.*

1. *$i_{L/K}$ is injective.*
2. *If $\mathfrak{a} \in I_K$ is an ideal in R_K then $K \cap i_{L/K}(\mathfrak{a}) = \mathfrak{a}$.*[4]
3. *$N_{L/K}(i_{L/K}(\mathfrak{a})) = \mathfrak{a}^{[L:K]}$ for all $\mathfrak{a} \in I_K$.*
4. *If L/K is Galois then*

$$i_{L/K}(N_{L/K}(\mathfrak{A})) = \prod_{\sigma \in G(L/K)} \sigma(\mathfrak{A})$$

for all $\mathfrak{A} \in I_L$.

[4]Let us remark that the proof below shows this is true for general $\mathfrak{a} \in I_K$, provided one can verify that $K \cap i_{L/K}(\mathfrak{a})$ is also a fractional ideal, i.e. is finitely generated over R_K. We have chosen to avoid this technicality.

5. *For any* $\alpha \in L$

$$N_{L/K}(\alpha)R_K = N_{L/K}(\alpha R_L)$$

where the norm on the left hand side is the ordinary field norm.

Proof. Since $i_{L/K}$ is multiplicative, equation (4) gives 1.

Since $\mathfrak{a} \subset R_K$, $\mathfrak{a}' = K \cap i_{L/K}(\mathfrak{a}) \subset R_K$ and so is an ideal in R_K. Clearly $\mathfrak{a} \subset \mathfrak{a}'$. It follows that there is an ideal $\mathfrak{b}$ in R_K so that $\mathfrak{a} = \mathfrak{a}'\mathfrak{b}$. Hence $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}'$ and so

$$i_{L/K}(\mathfrak{a})i_{L/K}(\mathfrak{b})^{-1} = i_{L/K}(\mathfrak{a}\mathfrak{b}^{-1}) = i_{L/K}(\mathfrak{a}') \subset i_{L/K}(\mathfrak{a}).$$

Thus

$$i_{L/K}(\mathfrak{a}) \subset i_{L/K}(\mathfrak{a}\mathfrak{b}) \subset i_{L/K}(\mathfrak{a}).$$

Since $i_{L/K}$ is injective it follows that $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ so that $\mathfrak{a} = \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}'$.

As $N_{L/K}(i_{L/K}(\mathfrak{a}))$ and $\mathfrak{a}^{[L:K]}$ are both multiplicative in $\mathfrak{a}$ it suffices to verify that they agree on prime ideals. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the primes of L over K, with ramification numbers e_i and inertial degrees f_i, respectively. Then

$$N_{L/K}(i_{L/K}(\mathfrak{p})) = N_{L/K}(\mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_g^{e_g}) = \mathfrak{p}^{e_1 f_1 + \cdots e_g f_g} = \mathfrak{p}^{[L:K]}.$$

As above, it suffices to verify that 4 holds for prime ideals. Let $\mathfrak{P}$ be a prime of L, $\mathfrak{p} = \mathfrak{P} \cap K$ and $f = f(\mathfrak{P}|\mathfrak{p})$. Let $G = G(L/K)$, $H = G(\mathfrak{P})$ and $\sigma_1 H, \ldots, \sigma_g H$ be a complete list of the cosets of H in G. Then $\sigma_1(\mathfrak{P}), \ldots, \sigma_g(\mathfrak{P})$ is a complete list of the distinct primes of L over $\mathfrak{p}$ and $\mathfrak{p}R_L = (\sigma_1(\mathfrak{P}) \cdots \sigma_g(\mathfrak{P}))^e$, where $e = e(\mathfrak{P}|\mathfrak{p})$. Thus

$$i_{L/K}(N_{L/K}(\mathfrak{P})) = i_{L/K}(\mathfrak{p}^f) = (\sigma_1(\mathfrak{P}) \cdots \sigma_g(\mathfrak{P}))^{ef}.$$

But we also have

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) = \prod_{\tau \in H} \prod_{i=1}^{g} \sigma_i \tau(\mathfrak{P}) = \prod_{\tau \in H} \prod_{i=1}^{g} \sigma_i(\mathfrak{P}) = (\sigma_1(\mathfrak{P}) \cdots \sigma_g(\mathfrak{P}))^{ef}$$

since $|H| = ef$.

For 5, Let M/K be a Galois extension containing L. We start by noticing that for $\alpha \in L$ we have

$$N_{M/K}(\alpha R_M) = N_{L/K}(N_{M/L}(\alpha R_M)) = N_{L/K}(N_{M/L}(i_{M/L}(\alpha R_L))) = N_{L/K}((\alpha R_L))^{[M:L]} \tag{5}$$

by what we have already shown. Now Let $G = G(M/K)$, $H = G(M/L)$ and $\sigma_1 H, \ldots, \sigma_g H$ be a complete list of the cosets of H in G. By 4 we have

$$\begin{aligned} i_{M/K}(N_{M/K}(\alpha R_M)) &= \prod_{\sigma \in G} \sigma(\alpha R_M) \\ &= \left(\prod_{\sigma \in G} \sigma(\alpha) \right) R_M \\ &= N_{M/K}(\alpha) R_M \\ &= N_{L/K}(N_{M/L}(\alpha)) R_M \\ &= i_{M/K}((N_{L/K}(\alpha) R_K)^{[M:L]}). \end{aligned}$$

Since $i_{M/K}$ is injectve we must have, in conjunction with (5),

$$N_{L/K}((\alpha R_L))^{[M:L]} = N_{M/K}(\alpha R_M) = (N_{L/K}(\alpha) R_K)^{[M:L]}.$$

By unique factorization of ideals, we may remove the exponent $[M : L]$ to reach our conclusion. □

We will need the norm, injection and this proposition for what follows. We will also frequently make use of the next result without explicit mention.

Lemma 25. *If L/K is a cyclic extension of number fields with group $G = \langle\sigma\rangle$ of order n, $\mathfrak{p}$ is a prime of K (finite or infinite), $\mathfrak{P}$ is a prime of L over $\mathfrak{p}$ and $G(\mathfrak{P}) = \langle\sigma^g\rangle$, $g|n$, then $\mathfrak{P}, \sigma(\mathfrak{P}), \ldots, \sigma^{g-1}(\mathfrak{P})$ are all distinct and give all primes of L over $\mathfrak{p}$.*

Proof. Since G is generated by σ the elements $1, \sigma, \ldots, \sigma^{g-1}$ give a complete set of coset representatives for $G/G(\mathfrak{P})$. The result follows. □

Let L/K be an extension of number fields and $\mathfrak{m}$ a modulus for K. We can view $\mathfrak{m}$ as a modulus for L simply by writing each prime that divides $\mathfrak{m}$ as a product of primes in L, and then discarding any complex primes that might show up. We point out that if $\mathfrak{m}_0$ is the finite part of the K-modulus $\mathfrak{m}$ then $i_{L/K}(\mathfrak{m}_0)$ is the finite part of $\mathfrak{m}$ viewed as an L-modulus. This means that if $\mathfrak{m}$ as a K-modulus is divisible by all of the finite primes of K ramified in L then as an L-modulus $\mathfrak{m}$ is divisible by all finite primes of L that lie over ramified primes of K.

Now suppose that L/K is Galois with group G. Given a finite prime $\mathfrak{p}$ of K let $I(\mathfrak{p})$ denote the subgroup of I_L generated by only those primes $\mathfrak{P}|\mathfrak{p}$. $I(\mathfrak{p})$ is a G-module and we have an obvious isomorphism

$$I_L \cong \prod_{\mathfrak{p}} I(\mathfrak{p})$$

the product on the right really being the direct sum of abelian groups (i.e. only finitely many nontrivial terms are ever allowed at once). It is clear that the product action of G is the same as the usual action of G on I_L and so this is a G-isomorphism. If $\mathfrak{m}$ is a modulus for K viewed as a modulus for L then restriction of the above isomorphism gives an isomorphism

$$I_L^{\mathfrak{m}} \cong \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} I(\mathfrak{p}) = \prod_{\mathfrak{p}\in I_K^{\mathfrak{m}}} I(\mathfrak{p}).$$

Since the right hand side is a G-submodule of the full direct "sum", this shows that $I_L^{\mathfrak{m}}$ is a G-submodule of I_L as well.

Proposition 8. *Let L/K be a cyclic extension of number fields with group $G = \langle\sigma\rangle$. Let $\mathfrak{m}$ be a modulus of K divisible by all those finite primes of K that ramify in L. Then, for the G-module $I_L^{\mathfrak{m}}$ we have*

i. $\ker\ \Delta = i_{L/K}(I_K^{\mathfrak{m}})$

ii. $\text{im}\ N = i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}}))$

iii. $\ker\ N = \text{im}\ \Delta$

Proof. For any ideal $\mathfrak{A} \in I_L^{\mathfrak{m}}$ and any prime $\mathfrak{p} \in I_K^{\mathfrak{m}}$ let

$$\mathfrak{A}_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{A})} \in I(\mathfrak{p})$$

In words, $\mathfrak{A}_{\mathfrak{p}}$ is the contribution to $\mathfrak{A}$ made by primes of L lying over $\mathfrak{p}$. We have

$$\mathfrak{A} = \prod_{\mathfrak{p}\in I_K^{\mathfrak{m}}} \mathfrak{A}_{\mathfrak{p}}$$

the product on the right side being defined since only finitely many of the terms are nontrivial. Moreover, the factors $\mathfrak{A}_{\mathfrak{p}}$ uniquely determine $\mathfrak{A}$.

Since G acts on the groups $I(\mathfrak{p})$ independently, we see that $\mathfrak{A} \in \ker\ \Delta$ ($\text{im}\ \Delta, \ker\ \text{N}, \text{im}\ \text{N}$, resp.) if and only if $\mathfrak{A}_{\mathfrak{p}} \in \ker\ \Delta$ ($\text{im}\ \Delta, \ker\ \text{N}, \text{im}\ \text{N}$, resp.) for all $\mathfrak{p} \in I_K^{\mathfrak{m}}$.

Since G is generated by σ, we see that $\mathfrak{A}_{\mathfrak{p}} \in \ker\ \Delta$ if and only if $\mathfrak{A}_{\mathfrak{p}} = \tau\mathfrak{A}_{\mathfrak{p}}$ for all $\tau \in G$. Since G permutes the primes over $\mathfrak{p}$ transitively it is clear that the latter condition holds if and only if the exponents appearing on each prime in $\mathfrak{A}_{\mathfrak{p}}$ are identical. That is, if and only if

$$\mathfrak{A}_{\mathfrak{p}} = \left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\right)^{n(\mathfrak{p})} = i_{L/K}(\mathfrak{p}^{n(\mathfrak{p})})$$

since $\mathfrak{p} \in I_K^{\mathfrak{m}}$ is unramified in L. This together with the remarks above proves statement (i).

Statement (ii) is actually trivial since

$$N(\mathfrak{A}) = \prod_{\tau \in G} \tau\mathfrak{A} = i_{L/K}(N_{L/K}(\mathfrak{A})).$$

The preceding equation actually tells us that an ideal is in the kernel of N if and only if it is in the ideal of $N_{L/K}$. We have

$$N_{L/K}(\mathfrak{A}_{\mathfrak{p}}) = \prod_{\mathfrak{P}|\mathfrak{p}} = \mathfrak{p}^{f_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\mathfrak{A})}$$

where $f_{\mathfrak{p}} = f(\mathfrak{P}|\mathfrak{p})$ for any $\mathfrak{P}|\mathfrak{p}$. Hence, $\mathfrak{A}_{\mathfrak{p}} \in \ker N_{L/K}$ if and only if

$$\sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\mathfrak{A}) = 0.$$

So, suppose that we have integers $n(\mathfrak{P})$ so that

$$\sum_{\mathfrak{P}|\mathfrak{p}} n(\mathfrak{P}) = 0.$$

Fix a prime $\mathfrak{P}|\mathfrak{p}$ and let

$$m_i = \sum_{j=1}^{i} n(\sigma^{j-1}\mathfrak{P})$$

for $j = 1, \ldots, g-1$, where $G(\mathfrak{P}) = \langle \sigma^g \rangle$ as in Lemma 25. Let

$$\mathfrak{B}_{\mathfrak{p}} = \prod_{j=1}^{g-1} (\sigma^{j-1}\mathfrak{P})^{m_j}.$$

Then

$$\Delta(\mathfrak{B}_{\mathfrak{p}}) = \mathfrak{B}_{\mathfrak{p}}\sigma(\mathfrak{B}_{\mathfrak{p}})^{-1} = \mathfrak{P}^{m_1} \left(\prod_{j=2}^{g-1} (\sigma^{j-1}\mathfrak{P})^{m_j - m_{j-1}} \right) (\sigma^{g-1}\mathfrak{P})^{-m_{g-1}} = \left(\prod_{j=1}^{g-1} (\sigma^{j-1}\mathfrak{P})^{n(\mathfrak{P}_{j-1})} \right) (\sigma^{g-1}\mathfrak{P})^{-m_{g-1}}$$

But

$$m_{g-1} = \sum_{j=1}^{g} n(\sigma^{j-1}\mathfrak{P}) - n(\sigma^{g-1}\mathfrak{P}) = \sum_{\mathfrak{P}|\mathfrak{p}} n(\mathfrak{P}) - n(\sigma^{g-1}\mathfrak{P}) = -n(\sigma^{g-1}\mathfrak{P})$$

and so

$$\Delta(\mathfrak{B}_{\mathfrak{p}}) = \prod_{j=1}^{g} (\sigma^{j-1}\mathfrak{P})^{n(\mathfrak{P}_{j-1})} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{n(\mathfrak{P})}$$

If we apply this in the case $n(\mathfrak{P}) = v_{\mathfrak{P}}(\mathfrak{A})$ then we find that $\Delta(\mathfrak{B}_{\mathfrak{p}}) = \mathfrak{A}_{\mathfrak{p}}$. That is, $\mathfrak{A}_{\mathfrak{p}} \in \ker N$ if and only if $\mathfrak{A}_{\mathfrak{p}} \in \operatorname{im} \Delta$. As before, our earlier remarks allow us to conclude at this point that (iii) holds.

□

Corollary 13. *If L/K is a cyclic extension of number fields and $\mathfrak{m}$ is a modulus for K divisible by all the finite primes that ramify in L, then*

i. $H^0(I_L^{\mathfrak{m}}) = i_{L/K}(I_K^{\mathfrak{m}})/i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}})) \cong I_K^{\mathfrak{m}}/N_{L/K}(I_L^{\mathfrak{m}})$,

ii. $H^1(I_L^{\mathfrak{m}})$.

Hilbert's Theorem 90 is equivalent to the second half of the following analogous fact.

Proposition 9. *Let L/K be a cyclic extension of number fields. Then $H^0(L^*) = K^*/N_{L/K}(L^*)$ and $H^1(L^*) = 1$.*

We now construct a certain G-module which will be very useful for two of our computations. Let L/K be a Galois extension of number fields with group G. Let $\mathfrak{p}$ be a prime (finite or infinite) of K and let

$$A_{\mathfrak{p}} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathbb{Z} u_{\mathfrak{P}}$$

be the free $\mathbb{Z}$-module on the basis $u_{\mathfrak{P}}$, $\mathfrak{P}|\mathfrak{p}$. This is a G-module via the action

$$\sigma u_{\mathfrak{P}} = u_{\sigma\mathfrak{P}}$$

of an element $\sigma \in G$ on a the basis elements $u_{\mathfrak{P}}$. If G is cyclic then Lemma 25 tells us this G-module is isomorphic to that occurring in Propositon V.1.5 of [1] and hence

$$q(A_{\mathfrak{p}}) = \frac{g}{[L:K]} = \frac{1}{e_{\mathfrak{p}} f_{\mathfrak{p}}}$$

where $e_{\mathfrak{p}} = e(\mathfrak{P}|\mathfrak{p})$, $f_{\mathfrak{p}} = f(\mathfrak{P}|\mathfrak{p})$ for any $\mathfrak{P}|\mathfrak{p}$. An immediate consequence is that for a finite prime $\mathfrak{p}$ of K the G-module $I(\mathfrak{p})$ is clearly isomorphic to $A_{\mathfrak{p}}$ and hence

$$q(I(\mathfrak{p})) = \frac{1}{e_{\mathfrak{p}} f_{\mathfrak{p}}}.$$

Before we can deduce the second consequence (for infinite $\mathfrak{p}$) we need one more lemma.

Lemma 26. *Let L/K be Galois with group G and let $S_{L,\infty}$ denote the set of infinite primes of L. There exist units $w_{\mathfrak{P}} \in U_L$ indexed by the primes $\mathfrak{P} \in S_{L,\infty}$ such that*

i. $\tau w_{\mathfrak{P}} = w_{\tau\mathfrak{P}}$ for all $\tau \in G$ and $\mathfrak{P} \in S_{L,\infty}$;

ii. $\prod_{\mathfrak{P}\in S_{L,\infty}} w_{\mathfrak{P}} = 1$, and this is the only relation among these units;

iii. $W = \langle w_{\mathfrak{P}} \mid \mathfrak{P} \in S_{L,\infty} \rangle$ has finite index in U_L.

This is proven as Proposition V.2.3 in [1] and is (essentially) a consequence of one of the computations in the proof of Dirichlet's unit theorem.

We use this lemma and the modules $A_{\mathfrak{p}}$ to compute the Herbrand quotient of U_L.

Theorem 19. *Let L/K be a cyclic extension of number fields. Then*

$$q(U_L) = \frac{[L:K]}{2^{r_0}}$$

where r_0 is the number of infinite primes of K ramified in L.

Proof. For $\mathfrak{P} \in S_{L,\infty}$ let $w_{\mathfrak{P}}$ be as in the lemma. According to fact (i) the map

$$\begin{array}{rcccc} \displaystyle\bigoplus_{\mathfrak{p}\in S_{K,\infty}} A_{\mathfrak{p}} = \bigoplus_{\mathfrak{p}\in S_{K,\infty}} \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathbb{Z} u_{\mathfrak{P}} & \to & W \\ u_{\mathfrak{P}} & \mapsto & w_{\mathfrak{P}} \end{array}$$

is a surjective G-homomorphism. Fact (ii) tells us that its kernel is

$$B = \mathbb{Z}\left(\sum_{\mathfrak{P}\in S_{L,\infty}} u_{\mathfrak{P}}\right).$$

It follows that we have an exact G-module sequence

$$0 \to B \to \bigoplus_{\mathfrak{p}} A_{\mathfrak{p}} \to W \to 1$$

so that

$$q(B)q(W) = q\left(\bigoplus_{\mathfrak{p}} A_{\mathfrak{p}}\right) = \prod_{\mathfrak{p}} q(A_{\mathfrak{p}}).$$

Since G acts trivially on B one may easily verify that $q(B) = |G|^{-1} = [L : K]^{-1}$. Fact (iii) tells us that $q(W) = q(U_L)$ and so

$$q(U_L) = \frac{[L : K]}{\prod_{\mathfrak{p} \in S_{K,\infty}} e_{\mathfrak{p}} f_{\mathfrak{p}}}.$$

This gives the desired conclusion since $f_{\mathfrak{p}} = 1$ for all infinite primes and $e_{\mathfrak{p}}$ is either 2 or 1 according to whether or not $\mathfrak{p}$ is ramified in L. □

While this result is interesting in its own right, we actually need a slightly more general result. We will actually need to compute the Herbrand quotient of a subgroup of L^* lightly larger that U_L, which we now define.

Let S be a set of primes of L and let

$$L^S = \{\alpha \in L^* \mid \iota(\alpha) \text{ is divisible only by } \mathfrak{p} \in S\}.$$

This is the subgroup of S-units of L. It is a generalization of (and contains) the usual unit group U_L, since $U_L = L^S$ where $S = \emptyset$. L^S consists of the elements of L^* that are units locally at all primes outside S. Notice that the infinite primes contained in S actually have no impact on the definition of L^S.

As usual, let L/K now be a Galois extension of number fields with group G and let $\mathfrak{m}$ be a modulus for K viewed as a modulus for L. We define a homomorphism $j_{\mathfrak{m}} : I_L \to I_L^{\mathfrak{m}}$ on prime ideals by

$$j_{\mathfrak{m}}(\mathfrak{P}) = \begin{cases} \mathfrak{P} & \text{, if } \mathfrak{P} \nmid \mathfrak{m} \\ 1 & \text{, if } \mathfrak{P} | \mathfrak{m} \end{cases}$$

and extend it multiplicatively. It is not hard to show that the fact that the primes of $\mathfrak{m}$ as an L-modulus occur in G-orbits implies that $j_{\mathfrak{m}}$ is a G-homomorphism. We define a second G-homomorphism by composing $j_{\mathfrak{m}}$ with ι: $f_{\mathfrak{m}} : L^* \to I_L^{\mathfrak{m}}$, $f_{\mathfrak{m}} = j_{\mathfrak{m}} \circ \iota$.

An immediate consequence of these definitions is that if S is the set of primes that divide the finite part of the L-modulus $\mathfrak{m}$ then $L^S = \ker f_{\mathfrak{m}}$ is a G-module. Lemma V.2.2 of [1] tells us that in this case, if G is cyclic, then $q(L^S) = q(U_L)q(\ker j_{\mathfrak{m}})$. We have already computed the first quantity on the right hand side. In fact, we have also essentially computed the second Herbrand quotient as well.

Lemma 27.

$$q(\ker j_{\mathfrak{m}}) = \prod_{\mathfrak{p} | \mathfrak{m}_0} \frac{1}{e_{\mathfrak{p}} f_{\mathfrak{p}}}$$

Proof. This follows at once from our earlier computations as soon as we notice that

$$\ker j_{\mathfrak{m}} \cong \prod_{\mathfrak{p} | \mathfrak{m}_0} I(\mathfrak{p}).$$

□

Theorem 20. *Let L/K be a cyclc extension of number fields. Let $\mathfrak{m}$ be a modulus for K and assume that $\mathfrak{m}$ is divisible by all the infinite primes of K that ramifiy in L. Let S be the set of primes of L dividing the L-modulus $\mathfrak{m}$. Then*

$$q(L^S) = \frac{[L : K]}{\prod_{\mathfrak{p} | \mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}}.$$

Proof. This is merely a collection of the facts that we have proven up to this point. The only thing that should probably be pointed out is that we have required $\mathfrak{m}$ to be divisible by all of the infinite ramified primes simply so that the quantity 2^{r_0} of Theorem 19 is included here. □

Two comments are in order here. First, we have actually shown that for *any* modulus $\mathfrak{m}$ of K, $q(L^S)$ is finite. Theorem 20 simply states that with additional hypotheses on $\mathfrak{m}$ we actually get a nice formula for it. Second, notice that our computations of the cohomology groups $I_L^{\mathfrak{m}}$ required the modulus $\mathfrak{m}$ to be divisible by all of the ramified finite primes. The computation of $q(L^S)$ that we have just given requires $\mathfrak{m}$ to be divisible by all of the infinite ramified primes. Soon we will need to use both of these computations simultaneously, which means that we will need to require $\mathfrak{m}$ to be divisible by *all* ramified primes.

V.3

Let L/K be an extension of number fields and let $\mathfrak{m}$ be a modulus for K. This section of the text is dedicated to the computation of the norm index

$$a(\mathfrak{m}) = [K^* : N_{L/K}(L^*)K_{\mathfrak{m},1}]$$

under certain restrictions on the extension L/K and the modulus $\mathfrak{m}$. We won't go over the computation in depth, but rather simply provide proofs of some auxiliary facts that are useful here and elsewhere.

The following lemma is proven during the course of the proof of Lemma V.3.1 of [1] in the case that L/K is Galois. However, the general case is needed later, so we prove it here.

Lemma 28. *Let L/K be number fields and let $\mathfrak{m}$ be a modulus for K, viewed as a modulus for L as well. Then*

$$N_{L/K}(L_{\mathfrak{m},1}) \subset K_{\mathfrak{m},1}.$$

Proof. Let $\alpha \in L_{\mathfrak{m},1}$ and let $\mathfrak{p}$ be a prime dividing the K-modulus $\mathfrak{m}$ with exponent $n \in \mathbb{Z}^+$. We must show that $N_{L/K}(\alpha) \equiv^* 1 \pmod{\mathfrak{p}^n}$.

First suppose that $\mathfrak{p}$ is real (so that $n = 1$), corresponding to the embedding σ of K into $\mathbb{R}$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ denote the real extensions of $\mathfrak{p}$ to L and let $\mathfrak{P}_{r+1}, \mathfrak{P}_{r+s}$ denote the complex extensions. Since $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ occur in the L-modulus $\mathfrak{m}$, we know that α is positive at these primes. Hence $N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha) > 0$ for these primes. Since $K_{\mathfrak{p}} = \mathbb{R}$ and $L_{\mathfrak{P}_i} = \mathbb{C}$ for the remaining primes, we have $N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha) > 0$ for these as well. Hence

$$N_{L/K}(\alpha) = \prod_{i=1}^{r} N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha) \prod_{i=r+1}^{r+s} N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha) > 0$$

where the left hand side is viewed in $K_{\mathfrak{p}}$ via the embedding σ. This proves that $N_{L/K}(\alpha) \equiv^* 1 \pmod{\mathfrak{p}}$.

Now suppose that $\mathfrak{p}$ is a prime ideal of K. We pass to a finite Galois extension M of K containing L. Let $H = G(M/L)$ and let τ_i, $i = 1, \ldots, [L : K]$ be coset representatives for H in $G(M/K)$. Since $\mathfrak{p}^n R_L$ divides the L-modulus $\mathfrak{m}$, we may use the interpretation of Lemma 12 to write $\alpha = a/b$ with $a, b \in R_L$, prime to $\mathfrak{p}^n R_L$ and satisfying $a \equiv b \pmod{\mathfrak{p}^n R_L}$. Now $\mathfrak{p}^n R_L \subset \mathfrak{p}^n R_M$ and since M/K is Galois, $\sigma(\mathfrak{p}^n R_M) = \mathfrak{p}^n R_M$ for all $\sigma \in G(M/K)$. It follows that

$$\tau_i(a) \equiv \tau_i(b) \pmod{\mathfrak{p}^n R_M}$$

for all i. Since $N_{L/K}$ is given by multiplying together the τ_i, we find

$$N_{L/K}(a) \equiv N_{L/K}(b) \pmod{\mathfrak{p}^n R_M}.$$

Thus $N_{L/K}(a) - N_{L/K}(b) \in \mathfrak{p}^n R_M \cap K = \mathfrak{p}^n$ so that

$$N_{L/K}(a) \equiv N_{L/K}(b) \pmod{\mathfrak{p}^n}.$$

Finally, since aR_L is relatively prime to $\mathfrak{p}^n R_L$, and $N_{L/K}(aR_L) = N_{L/K}(a)R_K$, we see that $N_{L/K}(a)$ is relatively prime to $\mathfrak{p}$. The same conclusion holds for $N_{L/K}(b)$ as well and Lemma 12 allows us to conclude that $N_{L/K}(\alpha) = N_{L/K}(a)/N_{L/K}(b) \equiv^* 1 \pmod{\mathfrak{p}^n}$.

□

To simplify notation and presentation, we introduce the so-called higher unit groups. We do this as generally as possible so that our ideas will be applicable when dealing with number fields or with their completions.

Let R be a Dedekind domain with quotient field K and let $\mathfrak{p} \subset R$ be a nonzero prime ideal. Let $v_\mathfrak{p}$ denote the corresponding $\mathfrak{p}$-adic valuation. We define

$$U_\mathfrak{p}^{(0)} = U_\mathfrak{p} = R_\mathfrak{p}^* = \{\alpha \in K^* \ : \ v_\mathfrak{p}(\alpha) = 0\}$$

and for $n \in \mathbb{Z}^+$

$$U_\mathfrak{p}^n = 1 + R_\mathfrak{p}\mathfrak{p}^n = \{\alpha \in K^* \ : \ v_\mathfrak{p}(\alpha - 1) \geq n\}.$$

It is easy to verify that these are all groups and that $U_\mathfrak{p}^n \subset U_\mathfrak{p}^{n-1}$ for all $n \in Z^+$.

Let K be a number field and let $\mathfrak{p}$ be a prime ideal of K, $K_\mathfrak{p}$ the associated completion and $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation on either field. Let $\hat{R}_\mathfrak{p}$ and $\hat{\mathfrak{p}}$ denote the valuation ring and ideal (respectively) in $K_\mathfrak{p}$. If L/K is Galois, we let $\mathfrak{P}$ denote a fixed prime of L over $\mathfrak{p}$ and use "hats" in the same way to denote the objects in the associated completion. Recall that the decomposition group $G(\mathfrak{P})$ is isomorphic to the Galois group $G(L_\mathfrak{P}/K_\mathfrak{p})$, the isomorphism provided by lifting elements of $G(\mathfrak{P})$ to $L_\mathfrak{P}$. Since elements of $G(\mathfrak{P})$ preserve the $\mathfrak{P}$-adic valuation on L, their lifts do the same on $L_\mathfrak{P}$. It follows that $\tau(\hat{\mathfrak{P}}^n) = \hat{\mathfrak{P}}^n$ for all n and all $\tau \in G(L_\mathfrak{P}/K_\mathfrak{p})$. Hence $U_{\hat{\mathfrak{P}}}^{(n)}$ is a $G(\mathfrak{P})$-module for every integer $n \geq 0$. In fact, we can say a bit more.

Lemma 29. *Let everything be as above and let $e = e(\mathfrak{P}|\mathfrak{p})$. Then for any integer $n \geq 0$*

$$N_{L_\mathfrak{P}/K_\mathfrak{p}}(U_{\hat{\mathfrak{P}}}^{(n)}) \subset U_{\hat{\mathfrak{p}}}^{(n/e)}.$$

Proof. Since $U_{\hat{\mathfrak{P}}}^{(n)}$ is a $G(\mathfrak{P})$-module, we see that $N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha) \in U_{\hat{\mathfrak{P}}}^{(n)} \cap K_\mathfrak{p}$ for all $\alpha \in U_{\hat{\mathfrak{P}}}^{(n)}$. But since $ev_\mathfrak{p}(a) = v_\mathfrak{P}(a)$ for all $a \in K_\mathfrak{p}$, we have $U_{\hat{\mathfrak{P}}}^{(n)} \cap K_\mathfrak{p} = U_{\hat{\mathfrak{p}}}^{(n/e)}$. □

Lemma 30. *Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime ideal of K, $n \in \mathbb{Z}^+$ and let $\mathfrak{m} = \mathfrak{p}^n$. Let $\mathfrak{P}$ be any prime of L over $\mathfrak{p}$ and let $N_\mathfrak{p} = N_{L_\mathfrak{P}/K_\mathfrak{p}}$. Then*

$$\frac{K_\mathfrak{m}}{K_\mathfrak{m} \cap N_{L/K}(L^*)K_{\mathfrak{m},1}} \cong \frac{U_{\hat{\mathfrak{p}}}}{N_\mathfrak{p}(U_{\hat{\mathfrak{P}}})U_{\hat{\mathfrak{p}}}^{(n)}}.$$

Proof. We start with two observations. First, it follows from our definitions that $K_\mathfrak{m} = U_\mathfrak{p}$ and $K_{\mathfrak{m},1} = U_\mathfrak{p}^{(n)}$. Second, the quotient on the right above makes sense since $N_\mathfrak{p}(U_{\hat{\mathfrak{P}}}) \subset U_{\hat{\mathfrak{p}}}$ by the lemma.

Inclusion induces a homomorphism

$$U_\mathfrak{p} \to U_{\hat{\mathfrak{p}}}/U_{\hat{\mathfrak{p}}}^{(n)}$$

which is surjective. For, since $K_\mathfrak{p}$ is the completion of K, given $\alpha \in U_{\hat{\mathfrak{p}}}$ there is $a \in K^*$ so that $v_\mathfrak{p}(a-\alpha) \geq n$ and $v_\mathfrak{p}(a) = v_\mathfrak{p}(\alpha) = 0$. Then $a \in U_\mathfrak{p}$ and

$$v_\mathfrak{p}\left(\frac{a}{\alpha} - 1\right) = v_\mathfrak{p}(a - \alpha) \geq n$$

so that $a/\alpha \in U_{\hat{\mathfrak{p}}}$. We compose this surjection with the projection onto the quotient $U_{\hat{\mathfrak{p}}}/N_\mathfrak{p}(U_{\hat{\mathfrak{P}}})U_{\hat{\mathfrak{p}}}^{(n)}$ and claim that the kernel is precisely $U_\mathfrak{p} \cap N_{L/K}(L^*)U_\mathfrak{p}^{(n)}$.

It is clear that the kernel contains $U_\mathfrak{p}^{(n)}$. That the kernel also contains $U_\mathfrak{p} \cap N_{L/K}(L^*)$ is fairly straightforward. Let $\tau_1, \ldots, \tau_g$ be representatives for the right cosets of $G(\mathfrak{P})$ in $G(L/K)$. Then for any $\alpha \in L^*$ we have

$$N_{L/K}(\alpha) = \prod_{\tau \in G(\mathfrak{P})} \prod_i \tau\tau_i(\alpha) = \prod_\tau \tau\left(\prod_i \tau_i(\alpha)\right) = N_\mathfrak{p}(\beta)$$

where $\beta = \prod_i \tau_i(\alpha)$. We have used the fact that $G(\mathfrak{P})$ can be identified with $G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ via lifting. This shows the every "global" norm is a "local" norm at any given prime ideal. Moreover, if $N_{L/K}(\alpha) \in U_{\mathfrak{p}}$ then, since $U_{\mathfrak{p}} \subset U_{\mathfrak{P}}$,

$$0 = v_{\mathfrak{P}}(N_{L/K}(\alpha)) = v_{\mathfrak{P}}\left(\prod_{\tau \in G(\mathfrak{P})} \prod_i \tau\tau_i(\alpha)\right) = \sum_{\tau \in G(\mathfrak{P})} v_{\mathfrak{P}}(\beta) = e_{\mathfrak{p}} f_{\mathfrak{p}} v_{\mathfrak{P}}(\beta),$$

since elements of $G(\mathfrak{P})$ preserve the $\mathfrak{P}$-adic valuation. This proves that $\beta \in U_{\mathfrak{P}}$ so that $U_{\mathfrak{p}} \cap N_{L/K}(L^*) \subset N_{\mathfrak{p}}(U_{\hat{\mathfrak{P}}})$, as claimed.

The reverse inclusion requires some effort. Write $\mathfrak{p}^n R_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{en}$ with $\mathfrak{P} = \mathfrak{P}_1$. Set $\tau_1 = 1$ and for each $i \neq 1$ choose $\tau_i \in G(L/K)$ with $\tau_i(\mathfrak{P}) = \mathfrak{P}_i$. Then the elements $\tau_1, \ldots, \tau_g$ give a complete set of representatives for the cosets of $G(\mathfrak{P})$. Let $\alpha \in U_{\mathfrak{p}}$ be in the kernel of our map. Then there is a $\beta_0 \in U_{\hat{\mathfrak{P}}}$ so that $\alpha N_{\mathfrak{p}}(\beta_0)^{-1} \in U_{\hat{\mathfrak{p}}}^{(n)}$. Using an earlier argument, we may choose $\beta \in U_{\mathfrak{P}} \subset L^*$ so that $\beta U_{\hat{\mathfrak{P}}}^{(ne)} = \beta_0 U_{\hat{\mathfrak{P}}}^{(ne)}$. The lemma above then tells us that $N_{\mathfrak{p}}(\beta) U_{\hat{\mathfrak{p}}}^{(n)} = N_{\mathfrak{p}}(\beta_0) U_{\hat{\mathfrak{p}}}^{(n)} = \alpha U_{\hat{\mathfrak{p}}}^{(n)}$.

Use the Approximation Theorem to find $\gamma \in L^*$ so that

$$\begin{aligned} \gamma &\equiv^* \beta \pmod{\mathfrak{P}^{ne}} \\ \gamma &\equiv^* 1 \pmod{\mathfrak{P}_i^{ne}}\ ,\ i \neq 1. \end{aligned}$$

That is, $\gamma \in U_{\mathfrak{P}_i}^{(ne)}$ for $i \neq 1$ and $\gamma/\beta \in U_{\mathfrak{P}}^{(ne)}$. If $\tau \in G(\mathfrak{P})$ and $i \neq 1$ we have

$$\tau\tau_i^{-1}\gamma \in U_{\tau\tau_i^{-1}\mathfrak{P}_j}^{(ne)} = U_{\mathfrak{P}}^{(ne)}$$

or, equivalently, $\tau\tau_i^{-1}\gamma \equiv^* 1 \pmod{\mathfrak{P}^{ne}}$. In the same way we conclude that $\tau(\gamma) \equiv^* \tau(\beta) \pmod{\mathfrak{P}^{ne}}$ for $\tau \in G(\mathfrak{P})$. Therefore

$$N_{L/K}(\gamma) = \prod_{\tau \in G(\mathfrak{P})} \prod_i \tau\tau_i^{-1}(\gamma) \equiv^* \prod_{\tau \in G(\mathfrak{P})} \tau(\beta) = N_{\mathfrak{p}}(\beta) \pmod{\mathfrak{P}^{ne}}.$$

This gives

$$\frac{N_{L/K}(\gamma)}{N_{\mathfrak{p}}(\beta)} \in U_{\mathfrak{P}}^{(ne)} \cap K \subset U_{\mathfrak{p}}^{(n)} \subset U_{\hat{\mathfrak{p}}}^{(n)}.$$

Finally, we have

$$N_{L/K}(\gamma) U_{\hat{\mathfrak{p}}}^{(n)} = N_{\mathfrak{p}}(\beta) U_{\hat{\mathfrak{p}}}^{(n)} = \alpha U_{\hat{\mathfrak{p}}}^{(n)}$$

and so

$$\frac{\alpha}{N_{L/K}(\gamma)} \in U_{\hat{\mathfrak{p}}}^{(n)} \cap K = U_{\mathfrak{p}}^{(n)}$$

which shows that

$$\alpha \in U_{\mathfrak{p}} \cap N_{L/K}(L^*) U_{\mathfrak{p}}^{(n)}.$$

□

V.4

This section of [1] proves the so-called Fundamental Equality for cyclic extensions. Before making any comments, let's recall the relevant notation. L/K denotes a cyclic extension of number fields, $G = G(L/K)$, $\mathfrak{m}$ is a modulus for K, viewed when necessary as a modulus for L in the usual way, and

$$C^{\mathfrak{m}} = \frac{I_K^{\mathfrak{m}}}{N_{L/K}(I_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})}.$$

This is a quotient of the ray class group and is consequently finite. We set

$$h_{\mathfrak{m}}(L/K) = |C^{\mathfrak{m}}|.$$

Recall that we have a G-module homomorphism $f_{\mathfrak{m}} = j_{\mathfrak{m}}\iota : L^* \to I_L^{\mathfrak{m}}$. If $\mathfrak{m}$ is divisible by all of the finite primes of K that ramify in L then, in view of our earlier computations, the induced a map on the 0th cohomology groups is

$$\begin{array}{rccc} f_0 : & \dfrac{K^*}{N_{L/K}(L^*)} & \to & \dfrac{i_{L/K}(I_K^{\mathfrak{m}})}{i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}}))} \\ & \alpha N_{L/K}(L^*) & \mapsto & j_{\mathfrak{m}}(\iota(\alpha))i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}})). \end{array}$$

Since $i_{L/K}$ is an injection, the right hand side above is isomorphic (in the natural way) to

$$\frac{I_K^{\mathfrak{m}}}{N_{L/K}(I_L^{\mathfrak{m}})}.$$

We compose f_0 with this isomorphism to simplify things somewhat. Notice that doing so will have no effect (up to isomorphism) on $\ker f_0$ or $\operatorname{cok} f_0$.

We seek to identify the composite map. We can define $j_{\mathfrak{m}} : I_K \to I_K^{\mathfrak{m}}$ in the same way that we defined it on I_L, namely we set

$$j_{\mathfrak{m}}(\mathfrak{p}) = \begin{cases} \mathfrak{p} & , \quad \text{if } \mathfrak{p} \nmid \mathfrak{m} \\ 1 & , \quad \text{if } \mathfrak{p} | \mathfrak{m} \end{cases}$$

and extend multiplicatively. By checking equality on prime ideals, one can easily verify that this version of $j_{\mathfrak{m}}$ is compatible with the previous in that $j_{\mathfrak{m}} \circ i_{L/K} = i_{L/K} \circ j_{\mathfrak{m}}$. It follows that for $\alpha \in K^*$ we have

$$j_{\mathfrak{m}}(\iota(\alpha)) = j_{\mathfrak{m}}(i_{L/K}(\iota(\alpha))) = i_{L/K}(j_{\mathfrak{m}}(\iota(\alpha)))$$

so that under the natural isomorphism we have the correspondence

$$j_{\mathfrak{m}}(\iota(\alpha))i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}})) = i_{L/K}(j_{\mathfrak{m}}(\iota(\alpha)))i_{L/K}(N_{L/K}(I_L^{\mathfrak{m}})) \leftrightarrow j_{\mathfrak{m}}(\iota(\alpha))N_{L/K}(I_L^{\mathfrak{m}}).$$

Hence, the composite map mentioned above, which we still denote by f_0, is given by

$$\begin{array}{rccc} f_0 : & \dfrac{K^*}{N_{L/K}(L^*)} & \to & \dfrac{I_K^{\mathfrak{m}}}{N_{L/K}(I_L^{\mathfrak{m}})} \\ & \alpha N_{L/K}(L^*) & \mapsto & j_{\mathfrak{m}}(\iota(\alpha))N_{L/K}(I_L^{\mathfrak{m}}). \end{array}$$

From f_0 we can construct the following somewhat intimidating-looking diagram. To keep it as simple as possible, we write $N = N_{L/K}$.

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \frac{N(L^*)K_{\mathfrak{m},1}}{N(L^*)} & \xrightarrow{f_0^*} & \frac{N(I_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})}{N(I_L^{\mathfrak{m}})} & \xrightarrow{p^*} & \ker d_4 & & \\ & & \downarrow{\scriptstyle d_5} & & \downarrow{\scriptstyle d_6} & & \downarrow{\scriptstyle d_7} & & \\ 1 & \longrightarrow \ker f_0 \longrightarrow & \frac{K^*}{N(L^*)} & \xrightarrow{f_0} & \frac{I_K^{\mathfrak{m}}}{N(I_L^{\mathfrak{m}})} & \xrightarrow{p} & \operatorname{cok} f_0 & \longrightarrow 1 & \\ & \downarrow{\scriptstyle d_1} & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \downarrow{\scriptstyle d_4} & & \\ 1 & \longrightarrow \ker g \longrightarrow & \frac{K^*}{N(L^*)K_{\mathfrak{m},1}} & \xrightarrow{g} & \frac{I_K^{\mathfrak{m}}}{N(I_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})} & \xrightarrow{p'} & \operatorname{cok} g & \longrightarrow 1 & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & 1 & & \end{array}$$

We make a few comments regarding the construction of this beast.

1. The map p is just projection onto the quotient and makes the middle row exact.

2. Since $j_{\mathfrak{m}} \circ \iota = \iota$ for elements of $K_{\mathfrak{m}}$, we have $j_{\mathfrak{m}}(\iota(K_{\mathfrak{m},1})) \subset \iota(K_{\mathfrak{m},1})$. Hence f_0 maps $N(L^*)K_{\mathfrak{m},1}/N(L^*)$ to $N(I_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})/N(I_L^{\mathfrak{m}})$ and f_0^* is just the restriction of f_0.

3. The map d_5 is inclusion and d_2 is the map onto the associated quotient, composed with the natural isomorphism. Likewise, d_6 is inclusion and d_3 is (essentially) projection onto the quotient. So the middle two columns are exact.

4. g is the map induced on the quotients by f_0.

5. p' is projection onto the quotient and therefore the bottom row is exact.

6. d_1 is just the restriction of d_2, which maps $\ker f_0$ to $\ker g$ by a straightforward diagram chase. Another diagram chase shows that it is surjective and hence the left-most column is exact.

7. d_4 is induced by d_3 and is surjective since p, d_3, and p' are surjective. d_7 is inclusion, so the right-most column is also exact.

8. Finally, p^* is the restriction of p, which is defined on the groups shown by commutativity of the diagram.

Another diagram chase shows that p^* is onto and that $p^* f_0^* = 1$. Since f_0^* is clearly a surjection, this implies that $\ker d_4 = \text{im } p^* = \text{im } p^* f_0^* = 1$. This and the remarks above allow us to conclude that d_4 is an isomorphism. We have therefore proven the next

Lemma 31. *We have*

1. $\text{cok } f_0 \cong \text{cok } g$
2. $\ker g \cong \ker f_0 / \ker d_1$.

Before we go on, we pause for a few more remarks. First of all, in constructing the diagram above, the only information we used that was particular to our situation was the definition and surjectivity of f_0^*. The rest of the constructions and diagram chasing are *purely formal*. The Fundamental Equality is a statement about $h_{\mathfrak{m}}(L/K)$, the size of the group $C^{\mathfrak{m}}$, which appears in the bottom row of the diagram. The order of the group to the left of $C^{\mathfrak{m}}$ is $a(\mathfrak{m})$, which is computed in section V.3 of [1] under certain restrictions on $\mathfrak{m}$. It follows that

$$h_{\mathfrak{m}}(L/K) = |C^{\mathfrak{m}}| = |\text{cok } g||\text{im } g| = a(\mathfrak{m})\frac{|\text{cok } g|}{|\ker g|}$$

and the lemma above tells us that we should be able to compute the quantities on the right that involve g from the analogous quantities for f_0. The map f_0 arose from cohomology and one continues to use cohomology to study it. We won't go into those computations here since the presentation in [1] is adequate. We will, however, prove one more preliminary fact.

Lemma 32. *We have*

$$\ker d_1 \cong \frac{K_{\mathfrak{m},1} \cap \iota^{-1}(N(I_L^{\mathfrak{m}}))}{K_{\mathfrak{m},1} \cap N(L^*)}.$$

Proof. First of all, it is clear from our definitions that $\ker d_1 = \ker f_0 \cap \ker d_2 = \ker f_0 \cap \text{im } d_5$. Therefore, $\alpha N(L^*) \in \ker d_1$ if and only if $\alpha N(L^*) = \beta N(L^*)$ for some $\beta \in K_{\mathfrak{m},1}$ with $j_{\mathfrak{m}}(\iota(\beta)) \in N(I_L^{\mathfrak{m}})$. Since $j_m(\iota(\beta)) = \iota(\beta)$ for $\beta \in K_{\mathfrak{m}}$, we see that the latter conditions are equivalent to $\alpha N(L^*) = \beta N(L^*)$ for some $\beta \in K_{\mathfrak{m},1}$ with $\iota(\beta) \in N(I_L^{\mathfrak{m}})$. Therefore we have a surjective homomorphism

$$\begin{aligned} K_{\mathfrak{m},1} \cap \iota^{-1}(N(I_L^{\mathfrak{m}})) &\to \ker d_1 \\ \beta &\mapsto \beta N(L^*). \end{aligned}$$

The kernel is clearly $K_{\mathfrak{m},1} \cap \iota^{-1}(N(I_L^{\mathfrak{m}})) \cap N(L^*)$. The proof will be finished if we can prove that

$$K_{\mathfrak{m},1} \cap N(L^*) \subset K_{\mathfrak{m}} \cap N(L^*) \subset \iota^{-1}(N(I_L^{\mathfrak{m}})).$$

So, let $\alpha \in K_{\mathfrak{m}} \cap N(L^*)$. Then there is a $\beta \in L^*$ so that $\alpha = N(\beta) \in K_{\mathfrak{m}}$. This gives

$$\iota(\alpha) = j_{\mathfrak{m}}(\iota(\alpha)) = j_{\mathfrak{m}}(N(\beta)R_K) = j_{\mathfrak{m}}(N(\beta R_L)) = N(j_{\mathfrak{m}}(\beta R_L)) \in N(I_L^{\mathfrak{m}}).$$

We have used the fact that $j_{\mathfrak{m}} \circ N = N \circ j_{\mathfrak{m}}$, which is easily verified by checking it on prime ideals. □

We let

$$n(\mathfrak{m}) = |\ker d_1| = [K_{\mathfrak{m},1} \cap \iota^{-1}(N(I_L^{\mathfrak{m}})) : K_{\mathfrak{m},1} \cap N(L^*)].$$

It is a consequence of the Fundamental Equality that if L/K is cyclic then there is a modulus $\mathfrak{m}$ for K so that $n(\mathfrak{m}) = 1$. We can use this fact to prove the Hasse Norm Theorem. Before we state it, however, we need one more definition.

Let L/K be number fields and let $\mathfrak{p}$ be a prime of K (finite or infinite). Let $\alpha \in K$. We say that α is a a *local norm* at $\mathfrak{p}$ if there is a prime $\mathfrak{P}$ of L, $\mathfrak{P}|\mathfrak{p}$, and a $\beta \in L_{\mathfrak{P}}$ so that

$$\alpha = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta).$$

We say that α is a *global norm* from L if there is a $\beta \in L$ so that $\alpha = N_{L/K}(\beta)$.

Theorem 21 (Hasse Norm Theorem). *Let L/K be a cyclic extension of number fields. Then an element of K is a global norm from L if and only if it is a local norm at every prime of K.*

Proof. It is easy to see that every global norm is a local norm everywhere. Indeed, this is true for any Galois extension L/K. If $\alpha = N_{L/K}(\beta)$ and $\mathfrak{p}$ is a prime of K, let $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$. Let $\tau_1, \ldots, \tau_g$ be right coset representatives for the decomposition group $G(\mathfrak{P})$ in $G = G(L/K)$. Then

$$\alpha = N_{L/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta) = \prod_{\tau \in G(\mathfrak{P})} \tau\left(\prod_i \tau_i(\beta)\right) = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\left(\prod_i \tau_i(\beta)\right)$$

since $G(\mathfrak{P}) = G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

The proof of the converse follows easily from the next three facts.

1. If α is a local norm at every finite prime of K then it is the norm of an ideal in L, that is

   $$\iota(\alpha) = N_{L/K}(\mathfrak{a})$$

   for some $\mathfrak{a} \in I_L$.

2. If $\alpha \in K^*$ is a local norm at every prime of K and $\mathfrak{m}$ is a modulus for K then there is a $\gamma \in L^*$ so that

   $$\alpha N_{L/K}(\gamma) \in K_{\mathfrak{m},1}$$

3. If $\mathfrak{m}$ is a modulus for K then

   $$I_K^{\mathfrak{m}} \cap N_{L/K}(I_L) \subset N_{L/K}(I_L^{\mathfrak{m}}).$$

Assuming these for now (we prove them below) we complete the proof. Let $\alpha \in K^*$ be a local norm at every prime of K. Let $\mathfrak{a} \in I_L$ so that $\iota(\alpha) = N_{L/K}(\mathfrak{a})$. Let $\mathfrak{m}$ be any modulus for K so that $n(\mathfrak{m}) = 1$. Such moduli exist by the Fundamental Equality. Choose $\gamma \in L^*$ so that $\alpha N_{L/K}(\gamma) \in K_{\mathfrak{m},1}$. Then we have

$$\iota(\alpha N_{L/K}(\gamma)) = N_{L/K}(\mathfrak{a}) N_{L/K}(\gamma R_L) = N_{L/K}(\mathfrak{b})$$

where $\mathfrak{b} = \mathfrak{a}(\gamma R_L)$. Since $\alpha N_{L/K}(\gamma) \in K_{\mathfrak{m},1} \subset K_{\mathfrak{m}}$ we have $N_{L/K}(\mathfrak{b}) = \iota(\alpha N_{L/K}(\gamma)) \in I_K^{\mathfrak{m}}$. The third fact then implies that $\iota(\alpha N_{L/K}(\gamma)) \in N_{L/K}(I_L^{\mathfrak{m}})$. Hence

$$\alpha N_{L/K}(\gamma) \in K_{\mathfrak{m},1} \cap \iota^{-1}(N_{L/K}(I_L^{\mathfrak{m}})) = K_{\mathfrak{m},1} \cap N_{L/K}(L^*)$$

since $n(\mathfrak{m}) = 1$. It follows that $\alpha \in N_{L/K}(L^*)$, proving the theorem.

So now we must prove the three facts. The last is the easiest, so we start there. Let $\mathfrak{a} \in I_K^{\mathfrak{m}} \cap N_{L/K}(I_L)$. Then there is a $\mathfrak{b} \in I_L$ so that $\mathfrak{a} = N_{L/K}(\mathfrak{b}) \in I_K^{\mathfrak{m}}$. It follows that

$$\mathfrak{a} = j_{\mathfrak{m}}(\mathfrak{a}) = j_{\mathfrak{m}}(N_{L/K}(\mathfrak{b})) = N_{L/K}(j_{\mathfrak{m}}(\mathfrak{b})) \in N_{L/K}(I_L^{\mathfrak{m}}).$$

Now we prove the first fact. Let $\alpha \in K^*$ be an element that is a local norm at every finite prime of K. Let $\mathfrak{p}$ be a finite prime of K with associated valuation $v_{\mathfrak{p}}$. Let $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$ for which there

exists $\beta \in L_{\mathfrak{P}}$ for which $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta) = \alpha$. Let $f = f(\mathfrak{P}|\mathfrak{p})$. Since $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$, to show that $\iota(\alpha)$ is the norm of an ideal it is enough to show that $f|v_{\mathfrak{p}}(\alpha)$. One way to see this is to note that

$$\hat{\mathfrak{p}}^{v_{\mathfrak{p}}(\alpha)} = \alpha \hat{R}_{\mathfrak{p}} = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta)\hat{R}_{\mathfrak{p}} = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta \hat{R}_{\mathfrak{P}}) = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\hat{\mathfrak{P}}^t) = \hat{\mathfrak{p}}^{tf}$$

since $\hat{\mathfrak{P}}$ is the only prime in $\hat{R}_{\mathfrak{P}}$.

Finally, we prove the second fact, which is the hardest. Let $\alpha \in K^*$ be a local norm at every prime and let $\mathfrak{m}$ be any modulus for K. For each $\mathfrak{p}_i|\mathfrak{m}$ choose a prime $\mathfrak{P}_i|\mathfrak{p}_i$ so that there is a $\beta_i \in L^*_{\mathfrak{P}_i}$ with $\alpha = N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\beta_i)$. Let b_i be the exponent of $\mathfrak{p}_i$ in $\mathfrak{m}$ and $e_i = e(\mathfrak{P}_i|\mathfrak{p}_i)$. We now approximate each β_i with an element of L^*. We must treat the infinite and finite cases separately.

If $\mathfrak{P}_i$ is finite, let $n_i = v_{\mathfrak{P}_i}(\beta_i)$. As $L_{\mathfrak{P}_i}$ is the completion of L we can find a $\beta_i' \in L^*$ so that $v_{\mathfrak{P}_i}(\beta_i' = \beta_i) \geq b_i e_i + n_i$. Then

$$v_{\mathfrak{P}_i}\left(\frac{\beta_i'}{\beta_i} - 1\right) \geq b_i e_i$$

so that $\beta_i'/\beta_i \in U^{(b_i e_i)}_{\widehat{\mathfrak{P}_i}}$. By Lemma 29 we have $N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\beta_i'/\beta_i) \in U^{(b_i)}_{\widehat{\mathfrak{p}_i}}$.

Now we approximate the β_i with a single element of L^*. Using the approximation theorem we can find $\gamma \in L^*$ so that

$$\begin{aligned} \gamma &\equiv^* \beta_i' \pmod{\mathfrak{P}_i^{b_i e_i}} \\ \gamma &\equiv^* 1 \pmod{\mathfrak{P}^{b_i e_i}} \quad \text{for } \mathfrak{P}|\mathfrak{p}_i,\ \mathfrak{P} \neq \mathfrak{P}_i \end{aligned}$$

for all i for which $\mathfrak{p}_i$ is finite and so that, when $\mathfrak{p}_i$ is infinite, γ has the same sign as α at $\mathfrak{P}_i$ (if it's real) and γ is positive at all other real $\mathfrak{P}|\mathfrak{p}_i$. We claim that this is the γ we're after, i.e. $N_{L/K}(\gamma) \equiv^* \alpha \pmod{\mathfrak{p}_i^{b_i}}$ for all i.

First consider the case when $\mathfrak{p}_i$ is real. If $\mathfrak{P}_i$ is real then $N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\gamma) = \gamma$ has the same sign as α at $\mathfrak{p}_i$ and $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}_i}}(\gamma) > 0$ for all other $\mathfrak{P}|\mathfrak{p}_i$. Hence, since it is the product of the local norms, $N_{L/K}(\gamma)$ has the same sign at $\mathfrak{p}_i$ as α. If $\mathfrak{P}_i$ is complex then $\alpha = N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\beta_i)$ is positive at $\mathfrak{p}_i$ and we have arranged it in this case so that $N_{L/K}(\gamma)$ is positive at $\mathfrak{p}_i$ in this case as well. In any case, $\alpha \equiv^* N_{L/K}(\gamma) \pmod{\mathfrak{p}_i}$.

Now consider the finite $\mathfrak{p}_i$. Arguing as in the proof of Lemma 30, the congruence conditions on γ imply that

$$\frac{N_{L/K}(\gamma)}{N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\beta_i')} \in U^{(b_i)}_{\widehat{\mathfrak{p}_i}}.$$

But we have already seen that $N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\beta_i')/\alpha = N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}(\beta_i'/\beta_i) \in U^{(b_i)}_{\widehat{\mathfrak{p}_i}}$. From this we find that

$$\frac{N_{L/K}(\gamma)}{\alpha} \in U^{(b_i)}_{\widehat{\mathfrak{p}_i}} \cap K = U^{(b_i)}_{\mathfrak{p}_i}$$

which is the same as saying $N_{L/K}(\gamma) \equiv^* \alpha \pmod{\mathfrak{p}_i^{b_i}}$. □

V.5

The following propositions are standard results from Galois theory and their proofs can be found in any algebra text, e.g. [2].

Proposition 10. *Let L/K be a finite Galois extension of fields. Let E/K be an arbitrary extension. Then EL/E is Galois and restriction induces an isomorphism*

$$G(EL/E) \cong G(L/L \cap E).$$

Proposition 11. *Let K_i/K be finite Galois extensions for $i = 1, \ldots, n$. Then $L = K_1 \cdots K_n$ is Galois over K. Suppose further that $K_i \cap (K_1 \cdots K_{i-1}) = K$ for all i. Then the map*

$$G(L/K) \to \prod_{i=1}^{n} G(K_i/K)$$

given by restricting into each factor is an isomorphism.

Cyclotomic Extensions of Number Fields. For any positive integer m we let θ_m denote a primitive mth root of unity. If K is a number field, then $K(\theta_m)$ will be called a *cyclotomic extension* of K. Such extensions are important in the proof of the Artin Reciprocity Theorem. Since $\mathbb{Q}(\theta_m)/\mathbb{Q}$ is known to be abelian and $K(\theta_m) = K\mathbb{Q}(\theta_m)$, Proposition 10 tells us that $K(\theta_m)/K$ is abelian. A *cyclotomic subfield* of K will be any subfield of K that is contained in some cyclotomic extension of $\mathbb{Q}$. Since K has only finitely many subfields, there is an integer M so that $\mathbb{Q}(\theta_M)$ contains all of the cyclotomic subfields of K. One should think of $\mathbb{Q}(\theta_M)$ as containing all of the "old" cyclotomic information in K. If we adjoin roots of unity to K that "have nothing to do with M" then we get "new" cyclotomic information. That is essentially the content of the next series of lemmas. These are implicit in [1], and we encapsulate them here for easy reference.

Lemma 33. *Let K be a number field and M an integer so that every cyclotomic subfield of K is contained in $\mathbb{Q}(\theta_M)$. If $(m, M) = 1$ then restriction induces an isomorphism*

$$G(K(\theta_m)/K) \cong G(\mathbb{Q}(\theta_m)/\mathbb{Q}).$$

Proof. Since $K(\theta_m) = K\mathbb{Q}(\theta_m)$, the result follows from Proposition 10 since

$$\mathbb{Q}(\theta_m) \cap K \subset \mathbb{Q}(\theta_m) \cap \mathbb{Q}(\theta_M) = \mathbb{Q}.$$

□

Lemma 34. *Let K be a number field and M an integer so that every cyclotomic subfield of K is contained in $\mathbb{Q}(\theta_M)$. Suppose that $(m, n) = (mn, M) = 1$. Then*

$$K(\theta_m)K(\theta_n) = K(\theta_{mn}) \quad \textit{and} \quad K(\theta_m) \cap K(\theta_n) = K.$$

Proof. Since $(m, n) = 1$, $\theta_m\theta_n$ is a primitive mnth root of 1. Also, θ_{mn}^n is a primitive mth root of 1 and θ_{mn}^m is a primitive nth root of 1. It follows that

$$K(\theta_{mn}) \subset K(\theta_m)K(\theta_n) \subset K(\theta_{mn}).$$

Lemma 33 and standard facts about cyclotomic extensions of $\mathbb{Q}$ imply

$$\phi(mn) = [K(\theta_{mn}) : K] = [K(\theta_{mn}) : K(\theta_m)]\phi(m).$$

Consequently

$$[K(\theta_n) : K] = \phi(n) = [K(\theta_{mn}) : K(\theta_m)] = [K(\theta_m)K(\theta_n) : K(\theta_m)] = [K(\theta_n) : K(\theta_n) \cap K(\theta_m)]$$

where we have used Proposition 10 for the final equality. From this the conclusion of the lemma follows. □

Lemma 35. *Let L/K be a Galois extension of number fields and let M be an integer so that every cyclotomic subfield of L is contained in $\mathbb{Q}(\theta_M)$. Suppose that $m_1, \ldots, m_n$ are pairwise relatively prime and that $(m_1 \cdots m_n, M) = 1$. Then $E = L(\theta_{m_1}, \ldots, \theta_{m_n})$ is Galois over K and the map*

$$G(E/K) \to G(L/K) \times \prod_{i=1}^{n} G(K(\theta_{m_i})/K)$$

given by restricting onto each factor is an isomorphism.

Proof. Since $E = L(\theta_{m_1}, \ldots, \theta_{m_n}) = LK(\theta_{m_1}) \cdots K(\theta_{m_n})$, it is enough to show, by Proposition 11, that

$$\begin{aligned} K(\theta_{m_i}) \cap (K(\theta_{m_1}) \cdots K(\theta_{m_{i-1}})) &= K \text{ for all } i, \\ L \cap (K(\theta_{m_1}) \cdots K(\theta_{m_n})) &= K. \end{aligned}$$

Since K is a subfield of L and all cyclotomic subfields of L are contained in $\mathbb{Q}(\theta_M)$, the same is true of the cyclotomic subfields of K. Therefore, lemma 34 and induction show that $K(\theta_{m_1}) \cdots K(\theta_{m_{i-1}}) = K(\theta_{m_1 \cdots m_{i-1}})$. Another application of Lemma 34 then gives the first equality above.

Since $L(\theta_{m_1\cdots m_n}) = LK(\theta_{m_1\cdots m_n})$, Proposition 10 and Lemma 33 imply

$$\phi(m_1\cdots m_n) = [L(\theta_{m_1\cdots m_n}) : L] = [K(\theta_{m_1\cdots m_n}) : L \cap K(\theta_{m_1\cdots m_n})] \leq \phi(m_1\cdots m_n).$$

It follows that

$$K = L \cap K(\theta_{m_1\cdots m_n}) = L \cap (K(\theta_{m_1})\cdots K(\theta_{m_n})).$$

□

The statement of Artin's Lemma that we give below subsumes both V.5.5 and V.5.6 of [1]. We have stated it in the present manner for two reasons. First of all, the statement and proof of V.5.6 actually assume the statement and proof of V.5.5, so it seems natural to just stick them both together. Secondly, we have included the definition of the field F in our statement since its precise nature is used in the proof of the Reciprocity Theorem. Recall that two elements σ and τ of an abelian group are called *independent* if $\langle\sigma\rangle \cap \langle\tau\rangle = 1$.

Lemma 36 (Artin's Lemma). *Let L/K be a cyclic extension of number fields with group $G(L/K) = \langle\sigma\rangle$ and degree $n = [L : K]$. Let $s \in \mathbb{Z}^+$ and let $\mathfrak{p}$ be a prime ideal of K that is unramified in L. Then there exists $m \in \mathbb{Z}^+$, prime to s and $\mathfrak{p}$, so that*

a. $\mathfrak{p}$ is unramified in $E = K(\theta_m)$ and $\varphi_{E/K}(\mathfrak{p})$ has order divisible by n;

b. restriction onto each factor gives an isomorphism

$$G(LE/K) \to G(L/K) \times G(E/K);$$

c. there exists $\tau \in G(E/K)$ independent of $\varphi_{E/K}(\mathfrak{p})$ and with order also divisible by n.

If we let $H \subset G(LE/K)$ correspond to the subgroup $\langle(\sigma,\tau),\ (\varphi_{L/K}(\mathfrak{p}), \varphi_{E/K}(\mathfrak{p}))\rangle$ under the isomorphism of (b) and we set $F = (LE)^H$ then

d. $F(\theta_m) = L(\theta_m)$;

e. $\mathfrak{p}$ splits completely in F;

Proof. Let $a = |R_K/\mathfrak{p}|$ be the counting norm of $\mathfrak{p}$. Choose M so that all of the cyclotomic subfields of L (and hence of K) are contained in $\mathbb{Q}(\theta_M)$. According to Lemma 5.4 of [1] we can find an integer $m \geq 2$ and a positive integer b so that

i. $(m, Ms) = 1$;

ii. $(a, m) = 1$ and a has order divisible by n in $(\mathbb{Z}/m\mathbb{Z})^\times$;

iii. $(b, m) = 1$, b has order divisible by n in $(\mathbb{Z}/m\mathbb{Z})^\times$ and b is independent of a in $(\mathbb{Z}/m\mathbb{Z})^\times$.

If we let $E = K(\theta_m)$ then Lemma 35 tells us that

$$G(LE/K) \to G(L/K) \times G(E/K), \tag{6}$$

given by restriction onto each factor is an isomorphism, which is (b).

If $\mathfrak{p}$ divided m then we'd have $m \in \mathfrak{p} \cap \mathbb{Z} = (p)$. Since $p|a$ it would follow that $p|(a, m)$, a contradiction. This also shows that $(p) = \mathfrak{p} \cap \mathbb{Z}$ is unramified in $\mathbb{Q}(\theta_m)$ so that $\mathfrak{p}$ is unramified in $K\mathbb{Q}(\theta_m) = E$, by Lemma 10.

Let $\gamma = \varphi_{E/K}(\mathfrak{p})$. Then

$$\gamma = \varphi_{E/K}(\mathfrak{p}) = \varphi_{\mathbb{Q}(\theta_m)/\mathbb{Q}}(N_{K/\mathbb{Q}}(\mathfrak{p})) = \varphi_{\mathbb{Q}(\theta_m)/\mathbb{Q}}(a\mathbb{Z}) = \sigma_a.$$

Here we have used Proposition III.3.1 of [1] and the properties of the Artin map of $\mathbb{Q}(\theta_m)/\mathbb{Q}$ laid out above Proposition III.3.3 of [1]. Equality is understood to hold upon restriction of γ to $\mathbb{Q}(\theta_m)$ (which is precisely the isomorphism of Lemma 33). Also, σ_a is the element of $G(\mathbb{Q}(\theta_m)/\mathbb{Q})$ which carries θ_m to θ_m^a, which we

know has the same order as that of a in $(\mathbb{Z}/m\mathbb{Z})^\times$. In particular, (ii) tells us that γ has order divisible by n. We have therefore proven (a).

Let σ_b denote the element of $G(\mathbb{Q}(\theta_m)/\mathbb{Q})$ which carries θ_m to θ_m^b. Using the isomorphism of $G(\mathbb{Q}(\theta_m)/\mathbb{Q})$ with $(\mathbb{Z})/m\mathbb{Z})^\times$, fact (iii) tells us that σ_b has order divisible by n and is independent of σ_a. If we lift σ_b to an element τ under the isomorphism $G(E/K) \cong G(\mathbb{Q}(\theta_m)/\mathbb{Q})$ we find that τ has order divisible by n and is independent of the lift, γ, of σ_a. This proves (c).

Since E and L are both Galois over K and $\mathfrak{p}$ is unramified in both, we know from Lemma 9 that $\mathfrak{p}$ is unramified in their composite. It follows from properties of the Frobenius that $\varphi_{LE/K}(\mathfrak{p})$ maps to $(\varphi_{L/K}(\mathfrak{p}), \varphi_{E/K}(\mathfrak{p}))$ under the isomorphism 6. Therefore $\varphi_{LE/K}(\mathfrak{p})$ is an element of H and fixes F. Since $F \subset LE$, $\mathfrak{p}$ is unramified in F and properties of the Frobenius tell us that $\varphi_{F/K}(\mathfrak{p}) = \varphi_{LE/K}(\mathfrak{p})|_F = 1$,[5] and so $\mathfrak{p}$ splits completely in F. This is (e).

The composite $F(\theta_m) = FE$ is the fixed field in LE of the intersection $H \cap G(LE/E)$, by standard Galois theory. Under the isomorphism of 6 this maps to

$$\langle (\sigma, \tau),\ (\varphi_{L/K}(\mathfrak{p}), \varphi_{E/K}(\mathfrak{p}))\rangle \cap (G(L/K) \times 1).$$

We claim that this intersection is trivial and hence that $FE = LE$. To see that this is the case, let

$$(\sigma, \tau)^u (\varphi_{L/K}(\mathfrak{p}), \varphi_{E/K}(\mathfrak{p}))^v \in G(L/K) \times 1.$$

The independence of τ and $\varphi_{E/K}(\mathfrak{p})$ implies that $\tau^u = \varphi_{E/K}^v = 1$. Since both have order divisible by n, we must have $n|u$ and $n|v$. But $G(L/K)$ has order n and so $\sigma^u = \varphi_{L/K}(\mathfrak{p})^v = 1$ as well. Now (d) is proven. □

The properties of the fields E and F of Artin's Lemma are precisely what are needed to prove the Reciprocity Theorem. Recall that if L/K is an abelian extension of number fields and $\mathfrak{m}$ is a modulus for K divisible by all the finite primes of K that ramify in L, we say that the *reciprocity law* holds for $(L, K, \mathfrak{m})$ if $\iota(K_{\mathfrak{m},1}) \subset \ker \varphi_{L/K}$.

Theorem 22 (Artin Reciprocity for Cyclic Extensions). *Let L/K be a cyclic extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by all the finite primes of K that ramify in L. Suppose the fundamental equality $h_{\mathfrak{m}}(L/K) = [L : K]$ holds. Then the reciprocity law holds for $(L, K, \mathfrak{m})$.*

Proof. We will show that $\ker \varphi_{L/K}|_{I_K^{\mathfrak{m}}} \subset \iota(K_{\mathfrak{m},1}) N_{L/K}(I_L^{\mathfrak{m}})$. Surjectivity of the Artin map and the fundamental equality then imply that both groups have the same index in $I_K^{\mathfrak{m}}$ and so must be identical.

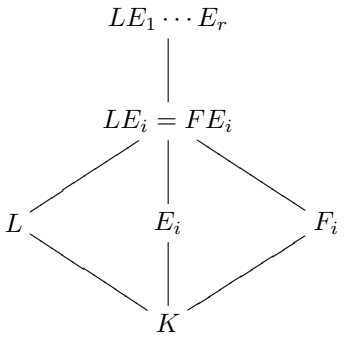
Let $\mathfrak{a} \in \ker \varphi_{L/K} \cap I_K^{\mathfrak{m}}$. Factor $\mathfrak{a}$ as a product of prime ideals in K:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}.$$

Since $\mathfrak{a} \in I_K^{\mathfrak{m}}$ and $\mathfrak{m}$ is divisible by all finite ramified primes, the $\mathfrak{p}_i$ are all unramified in L. We may therefore apply Artin's lemma to each. We do so as follows. Let M be an integer so that all cyclotomic subfields of L (and hence of K) lie in $\mathbb{Q}(\theta_M)$. Let m_1 be the integer produced by applying Artin's lemma with $s = M$ and $\mathfrak{p} = \mathfrak{p}_1$. Then let m_2 be the integer produced by applying Artin's lemma with $s = Mm_1$ and $\mathfrak{p} = \mathfrak{p}_2$. Continue in this manner: in general, given $m_1, \ldots, m_i$ let m_{i+1} be the integer produced by applying Artin's lemma with $s = Mm_1 \cdots m_i$ and $\mathfrak{p} = \mathfrak{p}_{i+1}$. We let E_i, τ_i, H_i and F_i denote the other objects produced by Artin's lemma at each stage. Also, let $n = [L : K]$ and $G(L/K) = \langle \sigma \rangle$.

[5]Here we are making use of the fact that F/K is Galois. This is trivial, since LE/K is abelian, so every subfield is also abelian.

We have the following diagram of field extensions.



We have arranged things so that Lemma 35 applies. All told, we end up with commutative diagrams

$$\begin{array}{ccc} G(LE_1 \cdots E_r/K) & \xrightarrow[\sim]{r_1} & G(L/K) \times \prod_{j=1}^{r} G(E_j/K) \\ \downarrow & & \downarrow p \\ G(LE_i/K) & \xrightarrow[\sim]{r_2} & G(L/K) \times G(E_i/K) \end{array}$$

for each i. The vertical map on the left is restriction, the maps r_1 and r_2 are products of restrictions onto each factor, and p is projection. We use this to identify in $G(LE_1 \cdots E_r)$ the group fixing F_i.

We see that $\epsilon \in G(LE_1 \cdots E_r)$ fixes F_i if and only if $\epsilon|_{LE_i}$ fixes F_i if and only if $\epsilon|_{LE_i} \in H_i$ if and only if $r_2(\epsilon|_{LE_i}) \in H_i' = \langle (\sigma, \tau_i),\ (\varphi_{L/K}(\mathfrak{p}_i), \varphi_{E_i/K}(\mathfrak{p}_i)) \rangle$. If we apply commutativity we find that this is true if and only if $p(r_1(\epsilon)) \in H_i'$ if and only if

$$r_1(\epsilon) \in H_i' \times \prod_{j \neq i} G(E_j/K).$$

So, if we let H_i'' denote the preimage of this group under r_1 then $F_i = (LE_1 \cdots E_r)^{H_i''}$ and $G(LE_1 \cdots E_r/F_i) = H_i''$.

Let $F = F_1 \cdots F_r$. Notice that $LE_1 \cdots E_r = LF$. We claim that $L \cap F = K$ so that $G(LF/F) \cong G(L/K)$ by Proposition 10. To see this, let $\epsilon = r_1^{-1}(1, \tau_1, \ldots, \tau_r)$ and let $\lambda = r_1^{-1}(\sigma, \tau_1, \ldots, \tau_r)$. Then ϵ fixes L and, since $\lambda \in H_i'' = G(LF/F_i)$ for every i, λ fixes F. It follows that $\lambda\epsilon^{-1}$ fixes $L \cap F$. But $r_1(\lambda\epsilon^{-1}) = (\sigma, 1, \ldots, 1)$. Thus σ fixes $L \cap F$ and since σ generates $G(L/K)$ we must have $L \cap F = K$.

Let $\varphi_{L/K}(\mathfrak{p}_i^{a_i}) = \sigma^{d_i}$ for some $d_i \geq 0$. Then

$$1 = \varphi_{L/K}(\mathfrak{a}) = \prod_i \sigma^{d_1}$$

so that $n | d = d_1 + \cdots d_r$.

Let $\mathfrak{m}'$ be a modulus for F divisible by all those finite primes that ramify in LF. Then the Artin map carries $I_F^{\mathfrak{m}'}$ onto $G(LF/F)$. We let $\mathfrak{m}'$ be any such modulus for F that is also divisible by the extension of $\mathfrak{m}$ to F as well as by the extension of $(m_1 \cdots m_n)$ to F. There is an ideal $\mathfrak{B} \in I_F^{\mathfrak{m}'}$ so that

$$\varphi_{LF/F}(\mathfrak{B}) = \sigma$$

equality being understood to hold after the left hand side has been restricted to L. Let $\mathfrak{b} = N_{F/K}(\mathfrak{B}) \in I_K^{\mathfrak{m}(m_1 \cdots m_n)}$. Since $\varphi_{LF/F} = \varphi_{L/K} \circ N_{F/K}$ by Proposition III.3.1, we conclude that $\varphi_{L/K}(\mathfrak{b}) = \sigma$. Being a norm from F, $\mathfrak{b}$ is also a norm from F_i for any i. Since $\mathfrak{p}_i$ splits completely in F_i it is also a norm. Therefore we can choose an ideal $\mathfrak{C}_i$ of F_i so that

$$N_{F_i/K}(\mathfrak{C}_i) = \mathfrak{p}_i^{a_i} \mathfrak{b}^{-d_i}.$$

Since $\mathfrak{p}_i$ and $\mathfrak{b}$ are prime to $\mathfrak{m}$ and to m_i, we can assume the same for $\mathfrak{C}_i$ (see fact (3) in the proof of the Hasse Norm Theorem). Lemma 9 then tells us that $\mathfrak{C}_i$ is unramified in $F_i(\theta_{m_i})$.

Now

$$\varphi_{LF_i/F_i}(\mathfrak{C}_i) = \varphi_{L/K}(N_{F_i/K}(\mathfrak{C}_i)) = \varphi_{L/K}(\mathfrak{p}_i)^{a_i}\varphi_{L/K}(\mathfrak{b}_i)^{-d_i} = \sigma^{d_i}\sigma^{-d_i} = 1.$$

By part (d) of Artin's lemma we have

$$F_i \subset LF_i \subset F_i(\theta_{m_i}).$$

Let $\mathfrak{m}_i''$ be the modulus for F_i that is the product of $\mathfrak{m}$ extended to F_i and $(m_i)p_\infty$ for $\mathbb{Q}$ extended to F_i (as usual, Lemma 9 tells us that $\mathfrak{m}_i''$ is divisible by all finite primes of F_i that ramify in $F_i(\theta_{m_i})$). The reciprocity law is known to hold for $(LF_i, F_i, \mathfrak{m}_i'')$ and we have already noted that $\mathfrak{C}_\mathfrak{i} \in I_{F_i}^{\mathfrak{m}_i''}$. Therefore, since $\mathfrak{C}_i \in \ker \varphi_{LF_i/F_i}$ we can find $\gamma_i \in F_i$ with $\gamma_i \equiv^* 1 \pmod{\mathfrak{m}_i''}$ and $\mathfrak{D}_i \in I_{LF_i}^{\mathfrak{m}_i''}$ so that

$$\mathfrak{C}_i = (\gamma_i)N_{LF_i/F_i}(\mathfrak{D}_i).$$

Taking norms to K yields

$$\mathfrak{p}_i^{a_i}\mathfrak{b}^{-d_i} = (N_{F_i/K}(\gamma_i))N_{LF_i/K}(\mathfrak{D}_i). \tag{7}$$

Since $\mathfrak{m}_i''$ is divisible by $\mathfrak{m}$ we know by Lemma 28 that

$$\alpha_i = N_{F_i/K}(\gamma_i) \in K_{\mathfrak{m},1}.$$

Finally, multiply together the equations (7) to get

$$\mathfrak{a}\mathfrak{b}^{-d} = \prod_i \mathfrak{p}_i^{a_i}\mathfrak{b}^{-d_i} = (\alpha_1 \cdots \alpha_r)N_{L/K}\left(\prod_i N_{LF_i/L}(\mathfrak{D}_i)\right).$$

Since $\mathfrak{m}_i''$ is divisible by $\mathfrak{m}$ and $\mathfrak{D}_i$ is prime to $\mathfrak{m}_i''$, we find that $\mathfrak{D}_i' = N_{LF_i/L}(\mathfrak{D}_i)$ is prime to $\mathfrak{m}$. Finally, since $d = nk$ for some k we have $\mathfrak{b}^d = N_{L/K}(i_{L/K}(\mathfrak{b}^k))$. We conclude that

$$\mathfrak{a} = (\alpha_1 \cdots \alpha_r)N_{L/K}\left(i_{L/K}(\mathfrak{b}^{d/n})\mathfrak{D}_1' \cdots \mathfrak{D}_r'\right) \in \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^\mathfrak{m})$$

which is what we sought out to show. □

This proof is no different in content than that given in [1]. We have just been a little more thorough with the details.

Let L/K be a cyclic extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by all the finite primes of K that ramify in L. We have just seen that the Fundamental Equality for the modulus $\mathfrak{m}$ implies that the reciprocity law holds for $(L, K, \mathfrak{m})$. This begs the question: when does the Fundamental Equality hold? Theorem V.4.4 of [1] asserts that it holds any time $\mathfrak{m}$ is divisible by all infinite ramified primes as well, and the exponents appearing on the finite primes are "sufficiently large." In most cases, knowing that we can find exponents that work for each prime appearing in $\mathfrak{m}$ is enough. But in other situations it is useful to have explicit lower bounds for exponents that guarantee the fundamental equality, and hence the reciprocity law, will hold.

Proposition 12. *Fix a number field K and a number $D > 0$. Let*

$$N = \max\{v_\mathfrak{p}(d) \ : \ \mathfrak{p} \text{ is a finite prime of } K, d \in \mathbb{Z}^+, d \leq D\} + [K : \mathbb{Q}].$$

If L/K is a cyclic extension, $[L : K] \leq D$, $\mathfrak{m}$ is a modulus for K divisible by all primes of K ramified in L, and the exponents on the finite primes dividing $\mathfrak{m}$ are all $> N$, then the fundamental equality $h_\mathfrak{m}(L/K) = [L : K]$ holds.

Proof. First note that since the d's occurring in the definition of N are bounded, they have only a finite number of prime divisors in K and so N is indeed finite. Let $\mathfrak{p}$ be a finite prime dividing $\mathfrak{m}$ with exponent n. Let $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $d = [L_\mathfrak{P} : K_\mathfrak{p}]$, where $\mathfrak{P}$ is any prime of L over $\mathfrak{p}$. Then we have

$$\begin{aligned} v_\mathfrak{p}(p) &= e(\mathfrak{p}|p) \leq [K : \mathbb{Q}] \\ d &= [L_\mathfrak{P} : K_\mathfrak{p}] \leq [L : K] \leq D. \end{aligned}$$

Thus

$$n > N \geq v_{\mathfrak{p}}(d) + [K : \mathbb{Q}] \geq v_{\mathfrak{p}}(d) + v_{\mathfrak{p}}(p)/(p-1).$$

If we now trace through the appropriate parts of the proof of the Fundamental Equality for Cyclic Extensions (Theorem V.4.4 of [1]) we reach the desired conclusion. Indeed, we find that the hypotheses of Corollary V.3.7 hold so that the conclusion of Theorem V.3.10 regarding the computation of the norm index $a(\mathfrak{m})$ is valid, and this in turn validates the proof of Theorem V.4.4. □

We are *not* asserting that the lower bound on the exponents we have just given is necessary for the fundamental equality: it is merely sufficient.

The general Artin Reciprocity Theorem is easily deduced from the cyclic case that we have proven above. It asserts that if L/K is abelian, $\mathfrak{m}$ is a modulus for K divisible by all the primes of K ramified in L and the exponents appearing on the finite primes in $\mathfrak{m}$ are sufficiently large, then the reciprocity law holds for $(L, K, \mathfrak{m})$. Again, we will find it useful to have an explicit condition on the exponents that is sufficient to guarantee the reciprocity law holds.

Proposition 13. *Fix a number field K and a number $D > 0$. Let*

$$N = \max\{v_{\mathfrak{p}}(d) \ : \ \mathfrak{p} \text{ is a finite prime of } K, d \in \mathbb{Z}^+, d \leq D\} + [K : \mathbb{Q}].$$

If L/K is an abelian extension, $[L : K] \leq D$, $\mathfrak{m}$ is a modulus for K divisible by all primes of K ramified in L, and the exponents on the finite primes dividing $\mathfrak{m}$ are all $> N$, then the reciprocity law holds for $(L, K, \mathfrak{m})$.

Proof. We begin as in the deduction of the general Reciprocity Theorem from the cyclic case: write

$$G(L/K) \cong C_1 \times \cdots \times C_n$$

with each C_i cyclic, let H_i be the subgroup of $G(L/K)$ corresponding to

$$\prod_{j \neq i} C_j$$

and set $L_i = L^{H_i}$. Then $L = L_1 \cdots L_n$ and $G(L_i/K) \cong C_i$. If a prime $\mathfrak{p}$ of K ramifies in L_i then it ramifies in L and so it divides $\mathfrak{m}$. Also, $[L_i : K] \leq [L : K] \leq D$ so we may apply the preceding proposition to conclude that the fundamental equality, and hence the reciprocity law, holds for $(L_i, K, \mathfrak{m})$, for every i. As in the proof of the Artin Reciprocity Theorem (V.5.8 of [1]) we conclude that the reciprocity law holds for $(L, K, \mathfrak{m})$. □

The next corollary tells us that if we bound the degree and the ramification of the abelian extensions of K under consideration, then we can find a *single* modulus that will make the reciprocity law hold.

Corollary 14. *Let K be a number field and $D > 0$. Fix a finite set S of primes of K and let*

$$\mathcal{S} = \{L \ : \ L/K \text{ is abelian and unramified outside } S, [L : K] \leq D\}.$$

Then there is a single modulus $\mathfrak{m}$ for K, divisible only by those primes in S, so that the reciprocity law holds for all $(L, K, \mathfrak{m})$ with $L \in \mathcal{S}$.

Proof. Let N be as in the proposition and let $\mathfrak{m}$ be the modulus whose prime divisors are exactly those in S, with exponent $N + 1$ on every finite prime. This $\mathfrak{m}$ works by the proposition. □

V.6

Here we collect a few comments on ideal groups and class fields. Given a number field K and a modulus $\mathfrak{m}$ for K recall that a group H of ideals is called a *congruence subgroup mod* $\mathfrak{m}$ if

$$\iota(K_{\mathfrak{m},1}) \subset H \subset I_K^{\mathfrak{m}}.$$

Suppose that $\mathfrak{n}$ is another modulus for K and that $\mathfrak{m}|\mathfrak{n}$. Then

$$\begin{aligned} I_K^{\mathfrak{n}} &\subset I_K^{\mathfrak{m}} \\ K_{\mathfrak{n},1} &\subset K_{\mathfrak{m},1} \end{aligned}$$

It follows that $H \cap I_K^{\mathfrak{n}}$ is a congruence subgroup mod $\mathfrak{n}$, called the *restriction* of H to $I_K^{\mathfrak{n}}$. Also, if H' is a congruence subgroup mod $\mathfrak{n}$ then $\iota(K_{\mathfrak{m},1})H'$ is a congruence subgroup mod $\mathfrak{m}$.

We define a relation on the set of congruence subgroups as follows. Let H_1 and H_2 be congruence subgroups mod $\mathfrak{m}_1$ and $\mathfrak{m}_2$ respectively. We say that H_1 and H_2 *have a common restriction* if there is a modulus $\mathfrak{m}$ so that

$$H_1 \cap I_K^{\mathfrak{m}} = H_2 \cap I_K^{\mathfrak{m}}.$$

In this case, we write $H_1 \sim H_2$. We remark that if $H_1 \cap I_K^{\mathfrak{m}} = H_2 \cap I_K^{\mathfrak{m}}$ and $\mathfrak{m}|\mathfrak{n}$ then $H_1 \cap I_K^{\mathfrak{n}} = H_2 \cap I_K^{\mathfrak{n}}$, since $I_K^{\mathfrak{n}} \subset I_K^{\mathfrak{m}}$. From this it follows easily that $\sim$ is an equivalence relation: see [1].

If H is a congruence subgroup mod $\mathfrak{m}$ and $\mathfrak{m}'$ is another modulus (not necessarily related to $\mathfrak{m}$) then it is not clear that $H \cap I_K^{\mathfrak{m}'}$ is a congruence subgroup mod $\mathfrak{m}'$. In particular, if $H_1 \equiv H_2$ as above then it may not be the case that $H_i \cap I_K^{\mathfrak{m}}$ is a restriction of H_i in the original sense of the word. But it is easy to remedy this situation: replace $\mathfrak{m}$ by a modulus $\mathfrak{m}'$ divisible by all of $\mathfrak{m}$, $\mathfrak{m}_1$ and $\mathfrak{m}_2$. Then $H_i \cap I_K^{\mathfrak{m}'}$ *is* a congruence subgroup mod $\mathfrak{m}'$ for $i = 1, 2$ and $H_1 \cap I_K^{\mathfrak{m}'} = H_2 \cap I_K^{\mathfrak{m}'}$. In particular if, in the definition of restriction, we require that the modulus $\mathfrak{m}$ be divisible by $\mathfrak{m}_1$ and $\mathfrak{m}_2$, then we get the same equivalence relation.

Part 1 of the following is implicit in [1].

Lemma 37. *1. If H_i are congruence subgroups mod $\mathfrak{m}_i$, $i = 1, 2$, and $H_1 \sim H_2$ then*

$$I_K^{\mathfrak{m}_1}/H_1 \cong I_K^{\mathfrak{m}_2}/H_2.$$

2. If H is a congruence subgroup mod $\mathfrak{m}$ and $\mathfrak{m}|\mathfrak{n}$ then

$$(H \cap I_K^{\mathfrak{n}})\iota(K_{\mathfrak{m},1}) = H.$$

3. If H_i are congruence subgroups mod $\mathfrak{m}_i$, $i = 1, 2$, and $H_1 \sim H_2$ then there is a congruence subgroup H mod $\mathfrak{m} = (\mathfrak{m}_1, \mathfrak{m}_2)$ so that

$$H \cap I_K^{\mathfrak{m}_i} = H_i \ , \ i = 1, 2.$$

Proof. Given the hypotheses of 1, the remarks preceding the lemma tell us we can find a modulus $\mathfrak{m}$ divisible by both $\mathfrak{m}_1$ and $\mathfrak{m}_2$ so that $H = H_1 \cap I_K^{\mathfrak{m}} = H_2 \cap I_K^{\mathfrak{m}}$. By Lemma V.6.1 of [1] we then have

$$I_K^{\mathfrak{m}_1}/H_1 \cong I_K^{\mathfrak{m}}/H \cong I_K^{\mathfrak{m}_2}/H_2.$$

2 and 3 are proven as Lemmas V.6.1 and V.6.2, respectively, of [1]. □

An equivalence class $\mathbb{H}$ of congruence subgroups is called an *ideal group*. The lemma above has several immediate consequences for ideal groups. Part 1 says that if $H \in \mathbb{H}$ is a congruence subgroup mod $\mathfrak{m}$ then $I_K^{\mathfrak{m}}/H$ depends on $\mathbb{H}$ only. Part 3 tells us that if $H_i \in \mathbb{H}$, $i = 1, 2$, are both congruence subgroups mod $\mathfrak{m}$ then there is a congruence subgroup H mod $(\mathfrak{m}, \mathfrak{m}) = \mathfrak{m}$ so that $H_i = H \cap I_K^{\mathfrak{m}}$ for $i = 1, 2$. That is, if $\mathbb{H}$ contains a congruence subgroup mod $\mathfrak{m}$ then it contains only one. If we combine this with part 2 we get the following consequence: if $H_i \in \mathbb{H}$, $i = 1, 2$, are congruence subgroups mod $\mathfrak{m}_i$ and $\mathfrak{m}_2|\mathfrak{m}_1$ then $H_1 = H_2 \cap I_K^{\mathfrak{m}_1}$ and $H_2 = \iota(K_{\mathfrak{m}_2,1})H_1$. Part 3 also tells us that if $H_i \in \mathbb{H}$ are congruence subgroups mod $\mathfrak{m}_i$, $i = 1, 2$, then there is a congruence subgroup mod $\mathfrak{m} = (\mathfrak{m}_1, \mathfrak{m}_2)$ in $\mathbb{H}$.

We use the notation $\mathbb{H}^{\mathfrak{m}}$ to denote the unique congruence subgroup in $\mathbb{H}$ defined mod $\mathfrak{m}$, if it exists. If we write $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$ we will mean that $\mathbb{H}$ does indeed contain a congruence subgroup mod $\mathfrak{m}$. The remarks above tell us that if $\mathbb{H}$ is an ideal group and $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$ then the group $I_K^{\mathfrak{m}}/\mathbb{H}^{\mathfrak{m}}$ depends (at least up to isomorphism) on $\mathbb{H}$ only. If $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$ and $\mathfrak{m}|\mathfrak{n}$ then $H = \mathbb{H}^{\mathfrak{m}} \cap I_K^{\mathfrak{n}}$ is a congruence subgroup mod $\mathfrak{n}$ and clearly $\mathbb{H}^{\mathfrak{m}} \sim H$. Therefore $\mathbb{H}^{\mathfrak{n}} = H = \mathbb{H}^{\mathfrak{m}} \cap I_K^{\mathfrak{n}}$. That is, the restriction of a congruence subgroup in an ideal group belongs to the same ideal group. We will use this observation frequently without explicit mention.

If $\mathbb{H}$ is an ideal group, the *conductor* of $\mathbb{H}$ is defined to be

$$\mathfrak{f} = \gcd\{\mathfrak{m} \mid \mathbb{H}^{\mathfrak{m}} \in \mathbb{H}\}.$$

Another consequence of the lemma above is the following.

Lemma 38. *The conductor* $\mathfrak{f}$ *of the ideal group* $\mathbb{H}$ *has the following properties.*

a. $\mathbb{H}^{\mathfrak{f}} \in \mathbb{H}$

b. $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$ *if and only if* $\mathfrak{f}|\mathfrak{m}$

c. If $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$ *then* $\mathbb{H}^{\mathfrak{m}} = I_K^{\mathfrak{m}} \cap \mathbb{H}^{\mathfrak{f}}$.

Proof. If $\mathbb{H}^{\mathfrak{m}_i} \in \mathbb{H}$ for $i = 1, 2$ then $\mathbb{H}^{\mathfrak{m}_1} \sim \mathbb{H}^{\mathfrak{m}_2}$ so part 3 of the lemma implies the existence of a congruence subgroup H mod $(\mathfrak{m}_1, \mathfrak{m}_2)$ so that $H \cap I_K^{\mathfrak{m}_i} = \mathbb{H}^{\mathfrak{m}_i}$ for $i = 1, 2$. Thus, $\mathbb{H}^{(\mathfrak{m}_1, \mathfrak{m}_2)} \in \mathbb{H}$. That is, the set $S(\mathbb{H}) = \{\mathfrak{m} \mid \mathbb{H}^{\mathfrak{m}} \in \mathbb{H}\}$ is closed under taking pairwise gcd's. It is easy to see that this means this set is closed under the taking of the gcd of any finite number of its elements. So, to show $\mathfrak{f} \in S(\mathbb{H})$ we need only show that $\mathfrak{f}$ is the gcd of a finite number of elements in $S(\mathbb{H})$. This isn't hard: choose any $\mathfrak{m} \in S(\mathbb{H})$ and let

$$S(\mathbb{H})_{\mathfrak{m}} = \{(\mathfrak{m}, \mathfrak{m}') \mid \mathfrak{m}' \in S(\mathbb{H})\}.$$

Then $S(\mathbb{H})_{\mathfrak{m}} \subset S(\mathbb{H})$ and it is easy to see that both sets have the same gcd. But $S(\mathbb{H})_{\mathfrak{m}}$ is finite, and so (a) follows.

(b) is clear from the definition of $\mathfrak{f}$.

As for (c), let $\mathbb{H}^{\mathfrak{m}} \in \mathbb{H}$. Since $\mathbb{H}^{\mathfrak{f}} \in \mathbb{H}$ and $\mathbb{H}$ is an equivalence class, and $\mathfrak{f}|\mathfrak{m}$, $\mathbb{H}^{\mathfrak{f}} \cap I_K^{\mathfrak{m}}$ is a congruence subgroup mod $\mathfrak{m}$ in $\mathbb{H}$. But we have already seen that such subgroups are unique and so we conclude that $\mathbb{H}^{\mathfrak{m}} = \mathbb{H}^{\mathfrak{f}} \cap I_K^{\mathfrak{m}}$.

□

Let $\mathbb{H}_1$ and $\mathbb{H}_2$ be ideal groups of K. We write $\mathbb{H}_1 \subset \mathbb{H}_2$ when there is a modulus $\mathfrak{m}$ for K so that $\mathbb{H}_i^{\mathfrak{m}} \in \mathbb{H}_i$ for $i = 1, 2$ and $\mathbb{H}_1^{\mathfrak{m}} \subset \mathbb{H}_2^{\mathfrak{m}}$. We note that our notation $\mathbb{H}_1 \subset \mathbb{H}_2$ is purely symbolic, since otherwise inclusion would be the same as equality, as we are dealing with equivalence classes. We also note that if $\mathbb{H}_1^{\mathfrak{m}} \subset \mathbb{H}_2^{\mathfrak{m}}$ holds for some modulus $\mathfrak{m}$ then it holds, by restriction, for all moduli that are multiples of $\mathfrak{m}$. Inclusion of ideal groups is a partial ordering, as is easily seen by using appropriate restrictions.

If $\mathbb{H}_1 \subset \mathbb{H}_2$ and $\mathbb{H}_i$ has conductor $\mathfrak{f}_i$ then $\mathbb{H}_1^{\mathfrak{m}} \subset \mathbb{H}_2^{\mathfrak{m}}$ holds for any modulus $\mathfrak{m}$ divisible by both $\mathfrak{f}_1$ and $\mathfrak{f}_2$. To see this, start with a modulus $\mathfrak{m}'$ for which $\mathbb{H}_1^{\mathfrak{m}'} \subset \mathbb{H}_2^{\mathfrak{m}'}$. By passing to restrictions we may assume that $\mathfrak{m}|\mathfrak{m}'$. Then, since $\mathbb{H}_i^{\mathfrak{m}} \in \mathbb{H}_i$,

$$\mathbb{H}_i^{\mathfrak{m}'} \iota(K_{\mathfrak{m},1}) = \mathbb{H}_i^{\mathfrak{m}}$$

for $i = 1, 2$, by our earlier remarks. This gives the desired conclusion.

Let K be a number field. The Artin Reciprocity Theorem allows us to associate and ideal group of K to each finite abelian extension of K. Let L/K be a finite abelian extension and let $\mathfrak{m}$ be a modulus for K, divisible by all finite primes of K ramified in L, so that the reciprocity law holds for $(L, K, \mathfrak{m})$. This means $\iota(K_{\mathfrak{m},1}) \subset \ker \varphi_{L/K} \cap I_K^{\mathfrak{m}} \subset I_K^{\mathfrak{m}}$ so that $\ker \varphi_{L/K} \cap I_K^{\mathfrak{m}}$ is a congruence subgroup mod $\mathfrak{m}$. It is shown in [1] that choosing any other modulus $\mathfrak{m}$ for which $(L, K, \mathfrak{m})$ has the reciprocity law results in an equivalent congruence subgroup, and so the kernels of the Artin map for the triples $(L, K, \mathfrak{m})$ for which the reciprocity law holds all belong to a single ideal group. We denote this ideal group by $\mathbb{H}(L/K)$ and call it the *class group* to the extension L/K. We call the conductor of the ideal group $\mathbb{H}(L/K)$ the *conductor* of the extension L/K and denote it by $\mathfrak{f}(L/K)$. It is worth noting that if $\mathbb{H}^{\mathfrak{m}}(L/K) \in \mathbb{H}(L/K)$ then $I_K^{\mathfrak{m}}/\mathbb{H}^{\mathfrak{m}}(L/K) \cong G(L/K)$. That is, the group canonically associated to $\mathbb{H}(L/K)$ is the Galois group of L/K.

If $\mathbb{H}$ is any ideal group and there is an abelian extension L/K so that $\mathbb{H} = \mathbb{H}(L/K)$ then we say that L is a *class field* to $\mathbb{H}$. The Existence Theorem, proven in section V.9 of [1], asserts that every ideal group has a class field, and the Classification Theorem tells us that the correspondence between abelian extensions L/K and the set of ideal groups given by $L \mapsto \mathbb{H}(L/K)$ is an inclusion reversing bijection. The Classification Theorem is the main result of class field theory.

V.7

Here we prove a few lemmas that are implicit in this section of [1], and clarify some of the explicitly made statements.

Lemma 39. *Let L/K be a Galois extension of number fields, let $\mathfrak{A} \in I_L$ and $\sigma \in G(L/K)$. Then*

$$N_{L/K}(\sigma\mathfrak{A}) = N_{L/K}(\mathfrak{A}).$$

Proof. By Proposition 7

$$i_{L/K}(N_{L/K}(\sigma\mathfrak{A})) = \prod_{\tau \in G(L/K)} \tau\sigma\mathfrak{A} = \prod_{\tau \in G(L/K)} \tau\mathfrak{A} = i_{L/K}(N_{L/K}(\mathfrak{A})).$$

We reach the desired conclusion by the injectivity of $i_{L/K}$. □

Let K be a number field. Let σ be an embedding of K over $\mathbb{Q}$. Let $\mathfrak{m}$ be a modulus for K. It is straightforward to show the following.

$$\begin{aligned}
\sigma(R_K) &= R_{\sigma(K)} \\
\sigma(I_K) &= I_{\sigma(K)} \text{ and } \sigma \text{ is a group isomorphism} \\
\mathfrak{p} \in I_K \text{ is prime} &\Leftrightarrow \sigma\mathfrak{p} \in I_{\sigma(K)} \text{ is prime} \\
\tau \text{ is a real (resp. complex) embedding of } K &\Leftrightarrow \tau\sigma^{-1} \text{ is a real (resp. complex) embedding of } \sigma(K) \\
\sigma(I_K^{\mathfrak{m}}) &= I_{\sigma(K)}^{\sigma\mathfrak{m}}.
\end{aligned}$$

The last equality deserves some comment. The above shows that σ provides a bijection between the set of primes of K (finite and infinite) and those of $\sigma(K)$. Since $\mathfrak{m}$ is just a product of primes, by $\sigma\mathfrak{m}$ we mean the modulus of $\sigma(K)$ obtained by mapping each prime that occurs in $\mathfrak{m}$ to the corresponding prime of $\sigma(K)$. With this definition, the final fact is easy to see.

Lemma 40. *Let L/K be an arbitrary extension of number fields. Let σ be an embedding of L over $\mathbb{Q}$. Then for any $\mathfrak{A} \in I_L$ we have*

$$\sigma(N_{L/K}(\mathfrak{A})) = N_{\sigma(L)/\sigma(K)}(\sigma(\mathfrak{A})).$$

Proof. $\sigma \circ N_{L/K}$ and $N_{\sigma(L)/\sigma(K)} \circ \sigma$ both give homomorphisms $I_L \to I_{\sigma(K)}$. Since I_L is free on the prime ideals, it therefore suffices to verify the equality for prime ideals only.

Let $\mathfrak{P}$ be a prime ideal of L and let $\mathfrak{p} = \mathfrak{P} \cap K$ be the prime under it in K. Then $\sigma(\mathfrak{P})$ is a prime of $\sigma(L)$ and $\sigma(\mathfrak{P}) \cap \sigma(K) = \sigma(\mathfrak{P} \cap K) = \sigma(\mathfrak{p})$ is the prime of $\sigma(K)$ under $\sigma(\mathfrak{P})$. We claim that

$$\begin{aligned}
e(\mathfrak{P}/\mathfrak{p}) &= e(\sigma(\mathfrak{P})/\sigma(\mathfrak{p})) \\
f(\mathfrak{P}/\mathfrak{p}) &= f(\sigma(\mathfrak{P})/\sigma(\mathfrak{p})).
\end{aligned}$$

The first equality follows from the fact that σ preserves multiplication of ideals, maps primes to primes, and $\sigma(R_L\mathfrak{p}) = R_{\sigma(L)}\sigma(\mathfrak{p})$. The second follows from the fact that σ induces an obvious isomorphism $R_L/\mathfrak{P} \cong R_{\sigma(L)}/\sigma(\mathfrak{P})$ which restricts to an isomorphism $R_K/\mathfrak{p} \cong R_{\sigma(K)}/\sigma(\mathfrak{p})$.

The rest of the proof follows immediately from these facts. Indeed, we have

$$\sigma(N_{L/K}(\mathfrak{P})) = \sigma(\mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}) = \sigma(\mathfrak{p})^{f(\sigma(\mathfrak{P})/\sigma(\mathfrak{p}))} = N_{\sigma(L)/\sigma(K)}(\sigma(\mathfrak{P})).$$

□

Lemma 41. *Let L/K be a Galois extension of number fields and let E be an intermediate field. Let $\mathfrak{P}$ be a prime ideal of L lying over an unramified prime of K and let $\sigma \in G(L/K)$. Then*

$$\sigma \left[\frac{L/E}{\mathfrak{P}}\right] \sigma^{-1} = \left[\frac{L/\sigma(E)}{\sigma(\mathfrak{P})}\right].$$

Proof. Let $\mathfrak{P}_E = \mathfrak{P} \cap E$. Then, as above, $\sigma(\mathfrak{P}_E) = \sigma(\mathfrak{P}) \cap \sigma(E)$ is the prime of $\sigma(E)$ under $\mathfrak{P}$. Let $\mathfrak{p} = \mathfrak{P} \cap K$, so that $\mathfrak{p}$ lies under both $\mathfrak{P}_E$ and $\sigma(\mathfrak{P}_E)$. We saw above that $f(\mathfrak{P}_E/\mathfrak{p}) = f(\sigma(\mathfrak{P}_E)/\sigma(\mathfrak{p})) = f(\sigma(\mathfrak{P}_E)/\mathfrak{p})$. Hence, by properties of the Frobenius we have

$$\sigma \left[\frac{L/E}{\mathfrak{P}}\right] \sigma^{-1} = \sigma \left[\frac{L/K}{\mathfrak{P}}\right]^{f(\mathfrak{P}_E/\mathfrak{p})} \sigma^{-1} = \left[\frac{L/K}{\sigma(\mathfrak{P})}\right]^{f(\mathfrak{P}_E/\mathfrak{p})} = \left[\frac{L/K}{\sigma(\mathfrak{P})}\right]^{f(\sigma(\mathfrak{P}_E)/\mathfrak{p})} = \left[\frac{L/\sigma(E)}{\sigma(\mathfrak{P})}\right].$$

□

Corollary 15. *Let L/K be a Galois extension of number fields and let E be an intermediate field so that $G(L/E)$ is abelian and normal in $G(L/K)$. Suppose that $\mathfrak{A} \in I_E$ is not divisible by any primes that ramify in L. Then for any $\sigma \in G(L/K)$*

$$\sigma \varphi_{L/E}(\mathfrak{A}) \sigma^{-1} = \varphi_{L/E}(\sigma(\mathfrak{A})).$$

Proof. The abelian and normality assumptions imply that both sides of this equation make sense and live in $G(L/E)$. Since both sides are multiplicative in $\mathfrak{A}$ it suffices, as usual, to verify that we have equality on prime ideals. But this is implied by the preceding lemma. □

Let us now consider some of the reduction steps in the proof of the Existence Theorem. The following is essentially Proposition V.7.2 of [1]. We state it so that we may comment on its proof.

Proposition 14. *Let E/K be cyclic and let H be a congruence subgroup mod $\mathfrak{m}$ of I_K. Let*

$$H_E = \{\mathfrak{A} \in I_E^{\mathfrak{m}} \mid N_{E/K}(\mathfrak{A}) \in H\}.$$

Then H_E is a congruence subgroup mod $\mathfrak{m}$. If the ideal group containing H_E has a class field over E then the ideal group containing H has a class field over K.

Partial. Since $N_{E/K}(E_{\mathfrak{m},1}) \subset K_{\mathfrak{m},1}$ and $\iota(K_{\mathfrak{m},1}) \subset H$ it follows from the definition of H_E that $\iota(E_{\mathfrak{m},1}) \subset H_E$, proving that H_E is a congruence subgroup mod $\mathfrak{m}$.

Let $\mathbb{H}$ be the ideal group containing H_E and let L/E be an abelian extension that is class field to $\mathbb{H}$. We want to start the proof by saying that, since $\mathbb{H} = \mathbb{H}(L/E)$, we have

$$H_E = \mathbb{H}^{\mathfrak{m}} = \ker \varphi_{L/E} \cap I_E^{\mathfrak{m}} = \iota(E_{\mathfrak{m},1}) N_{L/E}(I_L^{\mathfrak{m}}) \tag{8}$$

by the reciprocity law and the definition of $\mathbb{H}(L/E)$. However, $\mathfrak{m}$ was chosen arbitrarily, so there is no guarantee that the reciprocity law holds for $(L, E, \mathfrak{m})$. We'll replace $\mathfrak{m}$ by a different modulus in such a way that the ideal groups are unchanged and so that the reciprocity law does hold.

Choose a modulus $\mathfrak{m}'$ for E so that the reciprocity law holds for $(L, E, \mathfrak{m}')$. Find a modulus $\mathfrak{n}$ for K so that $\mathfrak{m}|\mathfrak{n}$ and $\mathfrak{m}'|\mathfrak{n}$ (when $\mathfrak{n}$ is extended to E). Then the reciprocity law still holds for $(L, E, \mathfrak{n})$ and so, since L is class field to $\mathbb{H}$

$$H_E \cap I_E^{\mathfrak{n}} = \mathbb{H}^{\mathfrak{m}} \cap I_E^{\mathfrak{n}} = \mathbb{H}^{\mathfrak{n}} = \ker \varphi_{L/E} \cap I_E^{\mathfrak{n}} = \iota(E_{\mathfrak{n},1}) N_{L/E}(I_L^{\mathfrak{n}}).$$

It is easy to verify that

$$H_E \cap I_E^{\mathfrak{n}} = \{\mathfrak{A} \in I_E^{\mathfrak{n}} \mid N_{E/K}(\mathfrak{A}) \in H \cap I_K^{\mathfrak{n}}\}.$$

Therefore, if we replace $\mathfrak{m}$ with $\mathfrak{n}$ and H with $H \cap I_K^{\mathfrak{n}}$ then the hypotheses of the proposition are unchanged, the ideal groups are the same as well, and equation (8) holds. From this point on the proof proceeds as in [1], making use of the lemmas above as needed. □

Now we come to the main reduction step. Consider the following two theorems.

Theorem 23 (Existence Theorem). *Let K be a number field and let $\mathbb{H}$ be an ideal group. Then there is an abelian extension L/K so that L is class field to $\mathbb{H}$, i.e. $\mathbb{H}(L/K) = \mathbb{H}$*

Theorem 24 (Reduced Theorem). *Let K be a number field that contains the nth roots of unity. Let $\mathbb{H}$ be an ideal group so that $I_K^{\mathfrak{m}}/\mathbb{H}^{\mathfrak{m}}$ has exponent n. Then there is an abelian extension L/K so that L is class field to $\mathbb{H}$, i.e. $\mathbb{H}(L/K) = \mathbb{H}$.*

Proposition 15 (Reduction Step). *The Reduced Theorem is equivalent to the Existence Theorem.*

This is proven as V.7.3 in [1]. We've just tried to clarify the statement a little. We also point out that in the statement of the Reduced Theorem one can assume that $n \geq 2$. For if $n = 1$ then $L = K$ serves as the necessary class field.

V.9

In this section we provide a slightly simplified proof of the Reduced Theorem. It still illustrates the main ideas of the proof given in [1], but avoids a few of the technical subtleties. We begin with two results that are essentially exercises in basic algebraic number theory.

Lemma 42. *Let K be a number field, $a \in R_K$, $n \geq 2$ an integer and α a root of $x^n - a$. If $L = K(\alpha)$ and $\mathfrak{p}$ is a prime of R_K not dividing na, then $\mathfrak{p}$ is unramified in L.*

Proof. Let $f(x) \in R_K[x]$ be the minimal polynomial for α over K and write $x^n - a = f(x)g(x)$ with $g(x) \in R_K[x]$. The product rule for differentiation yields $n\alpha^{n-1} = f'(\alpha)g(\alpha)$ and so

$$\pm N_{L/K}(g(\alpha))\Delta(\alpha) = N_{L/K}(f'(\alpha)g(\alpha)) = n^{[L:K]}N_{L/K}(\alpha)^{n-1}$$

by Theorem I.7.6 of [1]. If $\mathfrak{p}$ were ramified in L then we'd have $\Delta(\alpha) \in \Delta(L/K) \subset \mathfrak{p}$ so that $n^{[L:K]}N_{L/K}(\alpha)^{n-1} \in \mathfrak{p}$. We claim that this is impossible under our stated hypotheses.

If $n^{[L:K]}N_{L/K}(\alpha)^{n-1} \in \mathfrak{p}$ then, raising the quantity on the left to the nth power, we would have

$$(n^n a^{n-1})^{[L:K]} \in \mathfrak{p}.$$

Since $\mathfrak{p}$ is prime this would mean that $na \in \mathfrak{p}$, a contradiction. □

Corollary 16. *Let K be a number field, $\alpha \in K$, $n \geq 2$ an integer, β a root of $x^n - \alpha$ and $L = K(\beta)$. If $\mathfrak{p}$ is a prime of R_K not dividing n so that $\alpha \in U_\mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.*

Proof. Since $\alpha \in U_\mathfrak{p}$, we may write $\alpha = a/b$ with $a, b \in R_K$ both prime to $\mathfrak{p}$. Then $L = K(\beta) = K(b\beta)$ and $b\beta$ is a root of $x^n - ab^{n-1}$, to which we may apply the preceding lemma. □

Proof of the Reduced Theorem. Let K be a number field containing the nth roots of unity ($n \geq 2$) and let $\mathbb{H}$ be an ideal group over K with exponent n. Let $\mathfrak{m}$ be a modulus for K so that

1. $\mathbb{H}^\mathfrak{m} \in \mathbb{H}$;
2. $\mathfrak{m}$ is divisible by:
   a. all primes of K dividing n;
   b. all real primes of K;
   c. all primes dividing a collection of coset representatives $\{\mathfrak{a}_i\}$ of the ideal class group $C_K = I_K/\iota(K^*)$.
3. the exponents on the finite primes dividing $\mathfrak{m}$ are sufficiently large.

We will address point (3) momentarily. Let S be the set of primes dividing $\mathfrak{m}$ together with the complex primes of K and let

$$\begin{aligned} W_1 &= W = K^S K^n \\ W_2 &= K^S K^n \cap K_{\mathfrak{m},1} \end{aligned}$$

and notice that the definition of W depends only on the primes occurring in $\mathfrak{m}$, and not on the exponents with which they occur. Let $L = K(\sqrt[n]{W})$ and $L_2 = K(\sqrt[n]{W_2})$.

Lemma 43. *L and L_2 are finite abelian extensions of K and*

$$\begin{aligned} G(L/K) &\cong K^S/(K^S)^n \\ G(L_2/K) &\cong (K^S K^n \cap K_{\mathfrak{m},1})/(K^n \cap K_{\mathfrak{m},1}) \end{aligned}$$

Proof. Since

$$W/K^n = K^S K^n/K^n \cong K^S/K^S \cap K^n = K^S/(K^S)^n$$

which is finite of order $n^{|S|}$ by Corollary V.8.3 of [1] and

$$W_2 K^n/K^n \subset W/K^n$$

is also finite, Kummer theory tells us that both L and L_2 are abelian Kummer n-extensions of K and that we have the given group isomorphisms. □

Lemma 44. *The primes of K that ramify in L or L_2 all lie in S.*

Proof. For infinite primes this is obvious since S contains all the infinite primes of K. For finite primes this is a consequence of Corollary 16. If $\mathfrak{p} \notin S$ then $\alpha \in U_\mathfrak{p}$ and $\mathfrak{p}$ does not divide n, so that $\mathfrak{p}$ is unramified in $K(\sqrt[n]{\alpha})$. Both L and L_2 are (a finite number of) composites of fields of the form $K(\sqrt[n]{\alpha})$ with $\alpha \in K^S$, and these are all Galois over K since K contains the nth roots of unity, so the result follows. □

Lemma 45. *Let $\mathfrak{p}^t$ be the power of the finite prime $\mathfrak{p}$ occurring in $\mathfrak{m}$. Suppose that for all finite $\mathfrak{p}$ dividing $\mathfrak{m}$ we have $U_{\hat{\mathfrak{p}}}^{(t)} \subset U_{\hat{\mathfrak{p}}}^n$. Then all the primes in S split completely in L_2.*

Proof. Let $\mathfrak{p} \in S$ and $\mathfrak{P}|\mathfrak{p}$ in L_2. We will show that $[L_{2\mathfrak{P}} : K_\mathfrak{p}] = ef = 1$.

First suppose that $\mathfrak{p}$ is finite. Let $\alpha \in W_2$. Then $\alpha \in U_\mathfrak{p}^{(t)} \subset U_{\hat{\mathfrak{p}}}^{(t)} \subset U_{\hat{\mathfrak{p}}}^n$. Therefore

$$K_\mathfrak{p}(\sqrt[n]{\alpha}) = K_\mathfrak{p}$$

for all $\alpha \in W_2$. It follows that $L_{2\mathfrak{P}} = K_\mathfrak{p}(\sqrt[n]{W_2}) = K_\mathfrak{p}$.

Now suppose that $\mathfrak{p}$ is infinite. If $\mathfrak{p}$ is complex there is nothing to prove, so suppose that $\mathfrak{p}$ is real. Then $n = 2$ (as K has a real embedding and contains the nth root of unity). In this case, for $\alpha \in W_2$ we have $\alpha > 0$ at $\mathfrak{p}$ so that $K_\mathfrak{p}(\sqrt{\alpha}) = \mathbb{R}(\sqrt{\alpha}) = \mathbb{R} = K_\mathfrak{p}$. The conclusion follows as above. □

We now address point 3 on the size of the exponents appearing on the primes in $\mathfrak{m}$: we choose them so large that the reciprocity law holds for $(L, K, \mathfrak{m})$ (Lemma 44 guarantees this is possible) and so that the hypothesis of Lemma 45 holds (Proposition V.3.6 of [1] guarantees this is possible). In this case, we see that L_2/K is an unramified extension: the only primes that could potentially ramify lie in S, and Lemma 45 tells us none of these primes are actually ramified. It follows that the reciprocity law holds for $(L_2, K, 1)$.

Lemma 46. *Let $H^* = \iota(K_{\mathfrak{m},1}) N_{L/K}(I_L^\mathfrak{m})$ and $H_2^* = \iota(K^*) N_{L_2/K}(I_{L_2})$. Then*

$$\begin{aligned} I_K^\mathfrak{m}/H^* \cong &\quad G(L/K) &&\cong K^S/(K^S)^n \\ I_K/H_2^* \cong &\quad G(L_2/K) &&\cong (K^S K^n \cap K_{\mathfrak{m},1})/(K^n \cap K_{\mathfrak{m},1}). \end{aligned}$$

Proof. This is just a consequence of the reciprocity law and Lemma 43. □

Corollary 17. *We have*

$$[K^S K^n \cap K_{\mathfrak{m},1} : K^n \cap K_{\mathfrak{m},1}] = 1.$$

Proof. This will follow from the lemma if we show that $H_2^* = I_K$. To see this, let $\mathfrak{a} \in I_K$. By our choice of ideals in S, we know that there is an element $\alpha \in K^*$ and an ideal $\mathfrak{b} \in I(S)$ so that $\mathfrak{a} = (\alpha)\mathfrak{b}$. Therefore $I_K \subset \iota(K^*) I(S)$. But the primes in S split completely in L_2 and therefore $I(S) \subset N_{L_2/K}(I_{L_2})$. It follows that $I_K \subset H_2^*$. □

Let $H = \iota(K_{\mathfrak{m},1})(I_K^\mathfrak{m})^n$ have ideal group $\mathbb{H}'$. We claim that L/K is class field to $\mathbb{H}'$. For us L_2 is an auxiliary field introduced to facilitate the computation of the index $[K^S K^n \cap K_{\mathfrak{m},1} : K^n \cap K_{\mathfrak{m},1}]$. Since we have just seen that this quantity equals 1 we can actually conclude that $L_2 = K$.

If we can prove that L/K is class field to $\mathbb{H}'$ then we will be finished. Since $\mathbb{H}$ has exponent n we know that $(I_K^\mathfrak{m})^n \subset \mathbb{H}^\mathfrak{m}$ and hence $H \subset \mathbb{H}^\mathfrak{m}$. Therefore, we would have $\mathbb{H}(L/K) = \mathbb{H}' \subset \mathbb{H}$ and Proposition V.7.1 of [1] would tell us that $\mathbb{H}$ has a class field.

We are now in a position to begin our final computation. If we can show that $H = H^*$ we will be finished, for it will follow that

$$\mathbb{H}(L/K)^{\mathfrak{m}} = H^* = H = (\mathbb{H}')^{\mathfrak{m}}$$

so that $\mathbb{H}(L/K) = \mathbb{H}'$.

Since $I_K^{\mathfrak{m}}/H^* \cong K^S/(K^S)^n$ has exponent n, $(I_K^{\mathfrak{m}})^n \subset H^*$ and so we have $H \subset H^*$. From this and the Dirichlet-Hasse-Chevalley unit theorem it follows that

$$[I_K^{\mathfrak{m}} : H] \geq [I_K^{\mathfrak{m}} : H^*] = n^{|S|}.$$

with equality of indices if and only if $H = H^*$. We therefore need only prove that $[I_K^{\mathfrak{m}} : H] = n^{|S|}$.

Lemma 47. *We have*

$$\frac{K^*}{K^S K^n K_{\mathfrak{m},1}} \cong \frac{I_K^{\mathfrak{m}}}{H}.$$

Proof. Let f denote the composite of the maps

$$\begin{aligned} \iota : K^* &\rightarrow I_K \\ j_{\mathfrak{m}} : I_K &\rightarrow I_K^{\mathfrak{m}}, \end{aligned}$$

where $j_{\mathfrak{m}}$ was the map defined earlier which "forgets" the factors of an ideal that divide $\mathfrak{m}$. By our choice of the primes that divide $\mathfrak{m}$, given an ideal $\mathfrak{a} \in I_K^{\mathfrak{m}}$ we can find an ideal $\mathfrak{b} \in I(S)$ and an $\alpha \in K^*$ so that $\mathfrak{a} = (\alpha)\mathfrak{b}$. Then

$$f(\alpha) = j_{\mathfrak{m}}(\mathfrak{a}\mathfrak{b}^{-1}) = \mathfrak{a}$$

which proves that f is surjective. We compose f with the projection onto the quotient $I_K^{\mathfrak{m}}/H$ and show that the kernel of the resulting map is $K^S K^n K_{\mathfrak{m},1}$, yielding the desired isomorphism.

Let $\alpha \in K^*$ with $f(\alpha) \in H$. Write $\iota(\alpha) = \mathfrak{a}_0\mathfrak{a}_1$ with $\mathfrak{a}_0 \in I(S)$ and $\mathfrak{a}_1 \in I_K^{\mathfrak{m}}$ so that $f(\alpha) = \mathfrak{a}_1 \in H$. Then $\mathfrak{a}_1 = (\beta)\mathfrak{b}^n$ with $\beta \in K_{\mathfrak{m},1}$ and $\mathfrak{b} \in I_K^{\mathfrak{m}}$. As above, we may also write $\mathfrak{b} = (\theta)\mathfrak{b}_0$ with $\mathfrak{b}_0 \in I(S)$. Therefore

$$\iota(\alpha\beta^{-1}\theta^{-n}) = \mathfrak{a}_0\mathfrak{b}_0^n \in I(S)$$

so that

$$\alpha \in K^S K^n K_{\mathfrak{m},1}.$$

Conversely, it is clear that $f(K^S) = 1$, $f(K^n) \subset (I_K^{\mathfrak{m}})^n$ and $f(K_{\mathfrak{m},1}) = \iota(K_{\mathfrak{m},1})$ so that $f(K^S K^n K_{\mathfrak{m},1}) \subset \iota(K_{\mathfrak{m},1})(I_K^{\mathfrak{m}})^n$.

□

This lemma allows us to pass to our final reduction. We have

$$[I_K^{\mathfrak{m}} : H] = [K^* : K^S K^n K_{\mathfrak{m},1}] = \frac{[K^* : K^n K_{\mathfrak{m},1}]}{[K^S K^n K_{\mathfrak{m},1} : K^n K_{\mathfrak{m},1}]}.$$

We apply Lemma V.9.8 of [1] with $A = K^S K^n$, $B = K^n$ and $C = K_{\mathfrak{m},1}$ and Corollary 17 to get

$$n^{|S|} = [K^S K^n : K^n] = [K^S K^n K_{\mathfrak{m},1} : K^n K_{\mathfrak{m},1}][K^S K^n \cap K_{\mathfrak{m},1} : K^n \cap K_{\mathfrak{m},1}] = [K^S K^n K_{\mathfrak{m},1} : K^n K_{\mathfrak{m},1}].$$

Substituting this into the above we have

$$[I_K^{\mathfrak{m}} : H] = \frac{[K^* : K^n K_{\mathfrak{m},1}]}{n^{|S|}}.$$

The proof of the Reduced Theorem is finished by showing that $[K^* : K^n K_{\mathfrak{m},1}] = n^{2|S|}$. This final computation is (essentially) carried out in [1] on pages 212-214, and closely resembles the computation of the norm index $a(\mathfrak{n})$. We won't go through all of the details, but will simply fill in those that are left as exercises in [1].

For any modulus $\mathfrak{n}$ of K let $c(\mathfrak{n}) = [K^* : K^n K_{\mathfrak{n},1}]$.

Lemma 48. *If $\mathfrak{n}_1$ and $\mathfrak{n}_2$ are relatively primes then $c(\mathfrak{n}_1\mathfrak{n}_2) = c(\mathfrak{n}_1)c(\mathfrak{n}_2)$.*

Proof. The approximation theorem can be used to show that the diagonal map

$$K^* \to \frac{K^*}{K_{\mathfrak{n}_1,1}} \times \frac{K^*}{K_{\mathfrak{n}_2,1}}$$

is surjective with kernel $K_{\mathfrak{n}_1,1} \cap K_{\mathfrak{n}_2,1} = K_{\mathfrak{n}_1\mathfrak{n}_2,1}$. By composing with the obvious projections onto the quotients we get a surjective homomorphism

$$\frac{K^*}{K_{\mathfrak{n}_1\mathfrak{n}_2,1}} \to \frac{K^*}{K^n K_{\mathfrak{n}_1,1}} \times \frac{K^*}{K^n K_{\mathfrak{n}_2,1}}$$

whose kernel we now identify. If $\alpha \in K^*$ represents an element in the kernel then for $i = 1, 2$ there exists $\beta_i \in K^*$ so that $\alpha \equiv^* \beta_i^n \pmod{\mathfrak{n}_i}$. Use the approximation theorem again to find $\beta \in K^*$ with $\beta \equiv^* \beta_i \pmod{\mathfrak{n}_i}$ for $i = 1, 2$. Then $\alpha \equiv^* \beta^n \pmod{\mathfrak{n}_i}$ for $i = 1, 2$ so that $\alpha \equiv^* \beta^n \pmod{\mathfrak{n}_1\mathfrak{n}_2}$. That is, $\alpha \in K^n K_{\mathfrak{n}_1\mathfrak{n}_2,1}$ so that the map above yields an isomorphism

$$\frac{K^*}{K^n K_{\mathfrak{n}_1\mathfrak{n}_2,1}} \cong \frac{K^*}{K^n K_{\mathfrak{n}_1,1}} \times \frac{K^*}{K^n K_{\mathfrak{n}_2,1}},$$

proving the lemma. □

This lemma reduces the computation of $c(\mathfrak{n})$ to the case in which $\mathfrak{n}$ is divisible by a single prime. We consider the case in which $\mathfrak{n} = \mathfrak{p}^t$, $\mathfrak{p}$ a finite prime and fill in the details of the computation left as exercises in [1]. Specifically, we will be content to prove the following.

Lemma 49. *Let $\mathfrak{p}$ be a finite prime and let $\mathfrak{n} = \mathfrak{p}^t$. Then*

a. $[K^* : K^n K_{\mathfrak{n}}] = n$*;*

b. $c(\mathfrak{n}) = n[K_{\mathfrak{n}} : (K_{\mathfrak{n}})^n K_{\mathfrak{n},1}]$*;*

c. $K_{\mathfrak{n}}/(K_{\mathfrak{n}})^n K_{\mathfrak{n},1} \cong U_{\hat{\mathfrak{p}}}/U_{\hat{\mathfrak{p}}}^n U_{\hat{\mathfrak{p}}}^{(t)}$.

Proof. **(a):** We have $K_{\mathfrak{n}} = U_{\mathfrak{p}}$. Let $\pi \in K$ be the prime element in localization of the ring R_K at $\mathfrak{p}$. Then $K^* = \langle \pi \rangle \times U_{\mathfrak{p}}$ and $K^n K_{\mathfrak{n}} = \langle \pi^n \rangle \times U_{\mathfrak{p}}$ (internal direct products) and so

$$\frac{K^*}{K^n K_{\mathfrak{n}}} = \frac{\langle \pi \rangle \times U_{\mathfrak{p}}}{\langle \pi^n \rangle \times U_{\mathfrak{p}}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

(b): We have

$$c(\mathfrak{n}) = [K^* : K^n K_{\mathfrak{n}}][K^n K_{\mathfrak{n}} : K^n K_{\mathfrak{n},1}] = n[K^n K_{\mathfrak{n}} : K^n K_{\mathfrak{n},1}].$$

The map

$$K_{\mathfrak{n}} \to K^n K_{\mathfrak{n}}/K^n K_{\mathfrak{n},1}$$

given by $\alpha \mapsto \alpha K^n K_{\mathfrak{n},1}$ is clearly surjective with kernel $K_{\mathfrak{n}} \cap K^n K_{\mathfrak{n},1}$. Obviously $(K_{\mathfrak{n}})^n K_{\mathfrak{n},1} \subset K_{\mathfrak{n}} \cap K^n K_{\mathfrak{n},1}$, so we need only prove the reverse inclusion. Let $\alpha \in K_{\mathfrak{n}} \cap K^n K_{\mathfrak{n},1}$. Then $\alpha = \beta^n \gamma$ with $\gamma \in K_{\mathfrak{n},1}$. Since $\alpha \in K_{\mathfrak{n}}$ as well we see that $\beta^n \in K_{\mathfrak{n}}$ so that $\beta \in K_{\mathfrak{n}}$. Hence $\alpha = \beta^n \gamma \in (K_{\mathfrak{n}})^n K_{\mathfrak{n},1}$.

(c): Properties of completions imply that the composite map

$$U_{\mathfrak{p}} \hookrightarrow U_{\hat{\mathfrak{p}}} \to U_{\hat{\mathfrak{p}}}/U_{\hat{\mathfrak{p}}}^{(t)} \to U_{\hat{\mathfrak{p}}}/U_{\hat{\mathfrak{p}}}^n U_{\hat{\mathfrak{p}}}^{(t)}$$

is surjective (i.e. every element of $U_{\hat{\mathfrak{p}}}$ is a Cauchy sequence of elements in $U_{\mathfrak{p}}$). It is clear that $U_{\mathfrak{p}}^n U_{\mathfrak{p}}^{(t)}$ is contained in the kernel of this map. Conversely, if α is in the kernel then $\alpha \in \beta^n U_{\hat{p}}^{(t)}$ with $\beta \in U_{\hat{\mathfrak{p}}}$. Surjectivity of the map above implies that there is a $\beta_0 \in U_{\mathfrak{p}}$ so that $\beta_0 U_{\hat{\mathfrak{p}}}^{(t)} = \beta U_{\hat{\mathfrak{p}}}^{(t)}$. Then $\alpha \in \beta_0^n U_{\hat{\mathfrak{p}}}^{(t)}$ which yields

$$\alpha\beta_0^{-n} \in U_{\hat{\mathfrak{p}}}^{(t)} \cap K^* = U_{\mathfrak{p}}^{(t)}.$$

Hence $\alpha \in U_{\mathfrak{p}}^n U_{\mathfrak{p}}^{(t)}$ so that the kernel is precisely $U_{\mathfrak{p}}^n U_{\mathfrak{p}}^{(t)}$. Since $K_{\mathfrak{n}} = U_{\mathfrak{p}}$ and $K_{\mathfrak{n},1} = U_{\mathfrak{p}}^{(t)}$, we're finished. □

With these facts in hand, the computation of $c(\mathfrak{n})$ proceeds as in [1].

V.10

Lemma 50. *Let L/K be an abelian extension of number fields with group G and let $\sigma \in G$. Then the set of (unramified) primes of K with Frobenius equal to σ has density $1/|G|$.*

Proof. Let $\mathfrak{m}$ be a modulus for K so that the reciprocity law holds for $(L, K, \mathfrak{m})$. There is a unique coset $\mathbf{k} \in I_K^{\mathfrak{m}}/\mathbb{H}^{\mathfrak{m}}(L/K)$ so that $\varphi_{L/K}^{-1}(\sigma) = \mathbf{k}$. The set of primes in $\mathbf{k}$ has density $[I_K^{\mathfrak{m}} : \mathbb{H}^{\mathfrak{m}}(L/K)]^{-1} = [L : K]^{-1} = |G|^{-1}$ by Theorem V.10.3 of [1] and, aside from finitely many, this is the set of primes of K with Frobenius equal to σ. □

Theorem 25 (Tchebotarev Density Theorem). *Let L/K be a Galois extension of number fields with Galois group G and let $\sigma \in G$ have c conjugates in G. Then the set of (unramified) primes of K which have a prime divisor in L with Frobenius equal to σ has density $c/|G|$.*

Proof. Let T denote the set of primes of K, unramified in L, for which there exists a prime $\mathfrak{Q}$ of L dividing $\mathfrak{p}$ with

$$\left[\frac{L/K}{\mathfrak{Q}}\right] = \sigma.$$

Our goal is to show that $\delta(T) = c/|G|$.

Let E be the subfield of L fixed by $\langle\sigma\rangle$ so that $G(L/E) = \langle\sigma\rangle$. Let

$$S' = \{\mathfrak{P} \text{ of } E \ : \ \mathfrak{P} \cap K \text{ is unramified in } L, (L/E, \mathfrak{P}) = \sigma\}.$$

and let

$$S = \{\mathfrak{P} \in S' \ : \ f(\mathfrak{P}|\mathfrak{P} \cap K) = 1\}.$$

Aside from a finite set, S' is the set of primes of E unramified in L with Frobenius equal to σ. Lemma 50 therefore tells us that S' has density equal to $1/|\langle\sigma\rangle|$. Since the set of primes of E with relative degree 1 over K has density 1, it follows that S has density equal to $1/|\langle\sigma\rangle|$ as well.

It is not hard to show that

$$T = \{\mathfrak{P} \cap K \ : \ \mathfrak{P} \in S\}.$$

To see this suppose that $\mathfrak{p} = \mathfrak{P} \cap K$ with $\mathfrak{P} \in S$. Then, for any $\mathfrak{Q}$ of L over $\mathfrak{P}$, we have

$$\sigma = (L/E, \mathfrak{P}) = \left[\frac{L/E}{\mathfrak{Q}}\right] = \left[\frac{L/K}{\mathfrak{Q}}\right]^{f(\mathfrak{P}|\mathfrak{p})} = \left[\frac{L/K}{\mathfrak{Q}}\right]$$

by the change of base property of the Frobenius. Therefore $\mathfrak{p} \in T$. On the other hand, if $\mathfrak{p} \in T$, start by choosing $\mathfrak{Q}$ of L with

$$\left[\frac{L/K}{\mathfrak{Q}}\right] = \sigma.$$

Then $G(\mathfrak{Q}) = \langle\sigma\rangle$ so that $f(\mathfrak{Q}|\mathfrak{p}) = |G(\mathfrak{Q})| = |\langle\sigma\rangle|$. Let $\mathfrak{P} = \mathfrak{Q} \cap E$. Since $G(L/E) = \langle\sigma\rangle$ transitively permutes the primes of L over $\mathfrak{P}$ and $\mathfrak{Q}$ is such a prime, but is fixed by σ, $\mathfrak{Q}$ is the only prime of L over $\mathfrak{P}$. From this it follows that

$$f(\mathfrak{Q}|\mathfrak{P}) = [L : E] = |\langle\sigma\rangle| = f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P})f(\mathfrak{P}|\mathfrak{p})$$

so that $f(\mathfrak{P}|\mathfrak{p}) = 1$. Hence

$$\sigma = \left[\frac{L/K}{\mathfrak{Q}}\right] = \left[\frac{L/K}{\mathfrak{Q}}\right]^{f(\mathfrak{P}|\mathfrak{p})} = \left[\frac{L/E}{\mathfrak{Q}}\right] = (L/E, \mathfrak{P})$$

which shows that $\mathfrak{P} \in S$. Since $\mathfrak{p} = \mathfrak{P} \cap K$ we get the reverse inclusion.

Fix a prime $\mathfrak{p} \in T$, choose $\mathfrak{P} \in S$ with $\mathfrak{p} = \mathfrak{P} \cap K$ and fix $\mathfrak{Q}$ of L over $\mathfrak{P}$. Then

$$\sigma = (L/E, \mathfrak{P}) = \left[\frac{L/E}{\mathfrak{Q}}\right] = \left[\frac{L/K}{\mathfrak{Q}}\right]^{f(\mathfrak{P}|\mathfrak{p})} = \left[\frac{L/K}{\mathfrak{Q}}\right]$$

so that, among other things, $G(\mathfrak{Q}) = \langle\sigma\rangle$. Let $\tau_j\langle\sigma\rangle$, $j = 1, \ldots, t$, be the distinct left cosets of $\langle\sigma\rangle$ in G. Any prime of L over $\mathfrak{p}$ has the form $\tau_j\sigma^k\mathfrak{Q} = \tau_j\mathfrak{Q}$ for some j. Therefore, the primes of E over $\mathfrak{p}$ all have the form $\mathfrak{P}_j = \tau_j\mathfrak{Q} \cap E$. Notice that

$$(L/E, \mathfrak{P}_j) = \left[\frac{L/E}{\tau_j\mathfrak{Q}}\right] = \left[\frac{L/K}{\tau_j\mathfrak{Q}}\right]^{f(\mathfrak{P}_j|\mathfrak{p})} = \tau_j\sigma^{f(\mathfrak{P}_j|\mathfrak{p})}\tau_j^{-1}. \tag{9}$$

We claim that $\mathfrak{P}_j \in S$ if and only if $\tau_j \in C_G(\sigma)$. If $\mathfrak{P}_j \in S$ then $f(\mathfrak{P}_j|\mathfrak{p}) = 1$ so that equation (9) gives

$$\sigma = (L/E, \mathfrak{P}_j) = \tau_j\sigma\tau_j^{-1}.$$

Conversely, if $\tau_j \in C_G(\sigma)$, then τ_j commutes with σ and equation (9) gives

$$(L/E, \mathfrak{P}_j) = \sigma^{f(\mathfrak{P}_j|\mathfrak{p})}.$$

Therefore to show $\mathfrak{P}_j \in S$ it suffices to show that $f(\mathfrak{P}_j|\mathfrak{p}) = 1$. Since σ commutes with τ_j the group $G(L/E) = \langle\sigma\rangle$ fixes $\tau_j\mathfrak{Q}$. Hence, $\tau_j\mathfrak{Q}$ is the only prime of L over $\mathfrak{P}_j$ and so

$$f(\tau_j\mathfrak{Q}|\mathfrak{P}_j) = [L : E] = |\langle\sigma\rangle| = |G(\mathfrak{Q})| = f(\mathfrak{Q}|\mathfrak{p}) = f(\tau_j\mathfrak{Q}|\mathfrak{p}).$$

Multiplicativity of relative degrees gives us that $f(\mathfrak{P}_j|\mathfrak{p}) = 1$, as needed.

We claim that the assignment

$$\tau_j \in C_G(\sigma) \mapsto \tau_j Q \cap E = \mathfrak{P}_j$$

gives a bijection between the cosets of $\langle\sigma\rangle$ in $C_G(\sigma)$ and the primes of E in S over $\mathfrak{p}$. We have just seen that this map is well-defined and onto. We just need to verify that it is one-to-one. If $\mathfrak{P}_i = \mathfrak{P}_j$ then $\tau_i\mathfrak{Q}$ and $\tau_j\mathfrak{Q}$ lie over the same prime in E and therefore there is an element $\sigma^k \in \langle\sigma\rangle = G(L/E)$ so that $\sigma^k\tau_i\mathfrak{Q} = \tau_j\mathfrak{Q}$. Since σ commutes with τ_i and fixes $\mathfrak{Q}$ we find that $\tau_j^{-1}\tau_i \in G(\mathfrak{Q}) = \langle\sigma\rangle$. This means that τ_i and τ_j belong to the same left coset of $\langle\sigma\rangle$ and hence that $\tau_i = \tau_j$.

It follows from what we have just shown that for a given prime $\mathfrak{p} \in T$, the primes of S lying over $\mathfrak{p}$ are in one-to-one correspondence with the cosets of $\langle\sigma\rangle$ in $C_G(\sigma)$. That is, there are exactly

$$d = [C_G(\sigma) : \langle\sigma\rangle]$$

primes in S over $\mathfrak{p}$. Therefore

$$-\delta(S)\log(s-1) \sim \sum_{\mathfrak{P}\in S} N(\mathfrak{P})^{-s} = \sum_{\mathfrak{p}\in T}\sum_{\substack{\mathfrak{P}\in S\\ \mathfrak{P}|\mathfrak{p}}} N(\mathfrak{P})^{-s} = d\sum_{\mathfrak{p}\in T} N(\mathfrak{p})^{-s}$$

so that T has density and

$$\delta(T) = \frac{\delta(S)}{d} = \frac{1}{|\langle\sigma\rangle|}\frac{1}{[C_G(\sigma) : \langle\sigma\rangle]} = \frac{1}{|C_G(\sigma)|} = \frac{[G : C_G(\sigma)]}{|G|} = \frac{c}{|G|}.$$

□

References

[1] Janusz, G. J., Algebraic Number Fields (Second Edition), Graduate Studies in Mathematics **7**, American Mathematical Society (1996).

[2] Lang, S., Algebra (Third Edition), Addison-Wesley, (1993).

[3] Marcus, D. A., Number Fields, Springer-Verlag (1977).

[4] Narkiewicz, W., Elementary and Analytic Theory of Algebraic Numbers (Third Edition), Springer Monographs in Mathematics, Springer-Verlag, (2004).

[5] Neukirch, J., Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag (1999).