CHAPTER IX

KRONECKER'S THEOREM

For each prime p of $\mathbf{k}$, choose a non-negative integer m_p such that $m_p = 0$ for all but a finite number of primes, m_p is 0 or 1 for real finite primes and $m_p = 0$ for complex infinite primes. A *modulus* of $\mathbf{k}$ is a formal product

$$\mathbf{m} = \prod p^{m_p}$$

A closed subgroup H of finite index in $\mathbf{I_k}$ is open, so there exists some modulus $\mathbf{m}$ so that

$$H \supset \prod W_p(m_p) = W(\mathbf{m}).$$

Subgroup H is said to be defined modulo $\mathbf{m}$. If $\mathbf{m}'$ and $\mathbf{m}''$ are two moduli then the greatest common divisor $(\mathbf{m}', \mathbf{m}'')$ is the modulus $\mathbf{m}$ where $m_p = \min(m_p', m_p'')$. For finite and infinite primes, we have

$$W_p(m_p')W_p(m_p'') = W_p(m_p).$$

Therefore if H is defined modulo $\mathbf{m}'$ and $\mathbf{m}''$ then H is defined modulo $\mathbf{m} = (\mathbf{m}', \mathbf{m}'')$

If H is defined modulo some modulus, then there exists a modulus $\mathbf{m}$ so that H is defined modulo $\mathbf{m}$ and if H is defined modulo $\mathbf{w}$ then $\mathbf{m}$ divides $\mathbf{w}$. Modulus $\mathbf{m}$ is called the *conductor* of H.

LEMMA 9.1. *Take* $\mathbf{k} = \mathbf{Q}(\zeta)$ *where* ζ *is an* m*-th root of unity. Let* $\mathbf{m}$ *be the modulus* $(m)p_\infty$. *Then the kernel of* $\phi_{\mathbf{k}/\mathbf{Q}}$ *is* $\mathbf{Q}^* W(\mathbf{m})$.

PROOF. Suppose $\mathbf{i}$ in $\mathbf{I_Q}$ is in the kernel of $\phi_{\mathbf{k}/\mathbf{Q}}$. We can write $\mathbf{i} = \alpha\mathbf{j}$ where α is in $\mathbf{Q}^*$ and $\mathbf{j}$ is in $\prod_p W_p(0)$, and we can choose α so that $\mathbf{j}_{p_\infty}$ is positive. We want to show that $\mathbf{j}$ is in $W(\mathbf{m})$. We know that $\mathbf{j}$ is in $\ker\left(\phi_{\mathbf{k}/\mathbf{Q}}\right)$ since α is. By the Chinese remainder theorem, we can choose β in $\mathbf{Q}^*$ so that $\beta > 0$ and $\beta\mathbf{j}$ is in $W_p(m_p)$ when $m_p > 0$. We know $\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j}) = 1$, but we can also apply (3.2) to compute $\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j})$.

$$\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j}) = \prod_{p \nmid \mathbf{m}} \left(\frac{\mathbf{k} : \mathbf{Q}}{p}\right)^{b_p} \qquad \text{where } |\beta\mathbf{j}|_p = p^{-b_p}$$

Let $\beta = \beta_1/\beta_2$ where β_1 and β_2 are relatively prime positive integers. We want to show that $\beta_1 = \beta_2(\text{mod } m)$. We have

$$|\beta\mathbf{j}|_p = |\beta|_p = |\beta_1/\beta_2|_p = p^{-b'_p+b''_p} \qquad \text{where } |\beta_1|_p = p^{-b'_p} \text{ and } |\beta_2|_p = p^{-b''_p}.$$

Then

$$\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j}) = \prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{b'_p-b''_p} = \left(\prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{b'_p}\right)\left(\prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{b''_p}\right)^{-1}.$$

We have

$$\left(\prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{b'_p}\right)\zeta = \zeta^{\prod_{p\nmid\mathbf{m}} p^{b'_p}} = \zeta^{\beta_1}$$

and

$$\left(\prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{b''_p}\right)\zeta = \zeta^{\prod_{p\nmid\mathbf{m}} p^{b''_p}} = \zeta^{\beta_2}$$

since $\beta_1 > 0$ and $\beta_2 > 0$. This shows $\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j})$ is the result of applying $\zeta \to \zeta^{\beta_1}$ followed by the inverse of applying $\zeta \to \zeta^{\beta_2}$. Let $\beta_2\beta'_2 = 1(\text{mod } m)$. The inverse of $\zeta \to \zeta^{\beta_2}$ is $\zeta \to \zeta^{\beta'_2}$, so $\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j})\zeta = \zeta^{\beta_1\beta'_2}$. Since $\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j}) = 1$ we conclude that $\beta_1\beta'_2 = 1(\text{mod } m)$, and therefore $\beta_1 = \beta_2(\text{mod } m)$.

For each finite prime p dividing m, we have $\beta_1 = \beta_2(\text{mod } p^{m_p})$, so $\beta_1\beta_2^{-1}$ is in $W_p(m_p)$. Therefore β is in $W_p(m_p)$. Since $\beta\mathbf{j}$ is in $W_p(m_p)$, we conclude that $\mathbf{j}_p$ is in $W_p(m_p)$.

For finite primes p not dividing m, we have $\mathbf{j}_p$ in $W_p(0)$, and since $\mathbf{j}_{p_\infty}$ is positive we have $\mathbf{j}_{p_\infty}$ in $W_{p_\infty}(1)$. This shows that $\mathbf{j}$ is in $W(\mathbf{m})$, and therefore $\mathbf{i} = \alpha\mathbf{j}$ is in $\mathbf{Q}^*W(\mathbf{m})$. This shows that $\ker(\phi_{\mathbf{k}/\mathbf{Q}}) \subset \mathbf{Q}^*W(\mathbf{m})$.

The converse is easy. Suppose $\mathbf{j}$ is in $W(\mathbf{m})$. Applying (3.2) we have

$$\phi_{\mathbf{k}/\mathbf{Q}}(\mathbf{j}) = \prod_{p\nmid\mathbf{m}} \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^0 = 1$$

since $|\mathbf{j}|_p = 1$ for finite primes that do not divide m. This shows that $W(\mathbf{m}) \subset \ker(\phi_{\mathbf{k}/\mathbf{Q}})$, so $\mathbf{Q}^*W(\mathbf{m}) \subset \ker(\phi_{\mathbf{k}/\mathbf{Q}})$.

Proposition 9.2 (Kronecker's theorem). *Every abelian extension of the rational numbers is contained in a cyclotomic extension.*

Proof. Let $\mathbf{T}$ be an abelian extension of $\mathbf{Q}$. By Theorem 1, $\phi_{\mathbf{T}/\mathbf{Q}}$ is defined and $\ker\left(\phi_{\mathbf{T}/\mathbf{Q}}\right)$ is a closed subgroup of finite index in $\mathbf{I}_{\mathbf{Q}}$. Let $\mathbf{n}$ be the conductor of the kernel of $\phi_{\mathbf{T}/\mathbf{Q}}$. Then $\ker\left(\phi_{\mathbf{T}/\mathbf{Q}}\right)$ contains $\mathbf{Q}^* W(\mathbf{n})$. Choose $\mathbf{n}' = (n)p_\infty$ where n is the positive integer so that $(n) = \prod_{p \text{ finite}} p^{n_p}$. Then $\mathbf{n}$ divides $\mathbf{n}'$ because $\mathbf{n}$ is either (n) or $(n)p_\infty$. Put $\mathbf{k} = \mathbf{Q}(\zeta)$ where ζ is an n-th root of unity. Then, $\ker(\phi_{\mathbf{k}/\mathbf{Q}}) = \mathbf{Q}^* W(\mathbf{n}')$ by lemma 9.1,

$$\ker\left(\phi_{\mathbf{T}/\mathbf{Q}}\right) \supset \mathbf{Q}^* W(\mathbf{n}) \supset \mathbf{Q}^* W(\mathbf{n}') = \ker\left(\phi_{\mathbf{k}/\mathbf{Q}}\right),$$

so $\mathbf{T} \subset \mathbf{k}$ by proposition 2.15.