especially from the point of view of Kummer theory. In this section we sketch the basic set-up, leaving the details to the reader. The proofs are very similar to those in Chapter 10.

We start with a totally real field F. Let p be odd, let $K_0 = F(\zeta_p)$, and let K_∞/K_0 be the cyclotomic $\mathbb{Z}_p$-extension. Let M_∞ be the maximal abelian p-extension of K_∞ which is unramified outside p, and let

$$\mathscr{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty).$$

Then $\mathscr{X}_\infty$ is a Λ-module in the natural way (just as for $X = \mathrm{Gal}(L_\infty/K_\infty)$). Let M_n be the maximal abelian p-extension of K_n which is unramified outside p. Clearly $M_n \supseteq K_\infty$. We have

$$\mathrm{Gal}(M_n/K_\infty) \simeq \mathscr{X}_\infty/\omega_n \mathscr{X}_\infty,$$

where $\omega_n = \gamma_0^{p^n} - 1 = (1+T)^{p^n} - 1$. The proof is essentially the same as for Lemma 13.15, namely computing commutator subgroups, but in the present case we do not have to consider inertia groups. From Corollary 13.6 we know that

$$\mathrm{Gal}(M_n/K_0) \simeq \mathbb{Z}_p^{r_2 p^n + 1 + \delta_n} \times (\text{finite group}),$$

where $r_2 = r_2(K_0)$ and δ_n is the defect in Leopoldt's Conjecture (see Theorem 13.4). Therefore

$$\mathscr{X}_\infty/\omega_n \mathscr{X}_\infty \simeq \mathbb{Z}_p^{r_2 p^n + \delta_n} \times (\text{finite group}).$$

By Lemma 13.16, $\mathscr{X}_\infty$ is a finitely generated Λ-module, so

$$\mathscr{X}_\infty \sim \Lambda^a \oplus (\Lambda\text{-torsion})$$

for some $a \geq 0$.

Lemma 13.30. *δ_n is bounded, independent of n.*

1st edition Defective proof

Proof. Suppose $\delta_n > 0$ for some n. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis for $E_1 = E_1(K_n)$. We may assume $\varepsilon_{\delta_n+1}, \ldots, \varepsilon_r$ are independent and generate $\bar{E}_1$ over $\mathbb{Z}_p$. Then

$$\varepsilon_i = \prod_{j > \delta_n} \varepsilon_j^{a_{ij}}, \quad \text{with } a_{ij} \in \mathbb{Z}_p,$$

for $1 \leq i \leq \delta_n$. Let a'_{ij} be the nth partial sum of the p-adic expansion of a_{ij}. Let

$$\eta_i = \varepsilon_i \prod_j \varepsilon_j^{-a'_{ij}} \in E_1, \qquad 1 \leq i \leq \delta_n.$$

Then η_i is a p^nth power in $\bar{E}_1 \subseteq \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$, and $\eta_1, \ldots, \eta_{\delta_n}$ generate a subgroup $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$ of $K_n^\times/(K_n^\times)^{p^n}$. Since $\zeta_p \in K_0$ by assumption, $\zeta_{p^n} \in K_n$. Therefore the extension

$$K_n(\{\eta_i^{1/p^n}\})/K_n$$

has Galois group $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. Clearly this extension is unramified outside p. Since each η_i is a p^nth power in $U_{1,\mathfrak{p}}$ for each $\mathfrak{p}|p$, these primes split completely hence do not ramify. Therefore the Galois group X_n of the Hilbert p-class field of K_n has a quotient isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. In the decomposition of

1st edition, continued.

X, the terms of the form $\Lambda/(p^k)$ cannot account for this for large n. The term of the form $\bigoplus_j \Lambda/(g_j(T))$ can only yield $(\mathbb{Z}/p^n\mathbb{Z})^\lambda$, where $\lambda = \sum \deg g_j$. Therefore $\delta_n \le \lambda$. This completes the proof. $\square$

If $\zeta_p \notin K_0$, the lemma is still true. Simply adjoin ζ_p and use the easily proved fact that if $K \subseteq L$ then $\delta(K) \le \delta(L)$.

The above result perhaps could have been conjectured from Theorem 7.10 (although we already know $\delta_n = 0$ in that situation). Intuitively, the number δ_n should be approximately the number of occurrences of $L_p(1, \chi) = 0$ for K_n^+. Since each series $f(T, \theta)$ has only finitely many zeros,

$$L_p(1, \theta\psi) = f(\zeta_\psi(1 + q_0) - 1, \theta) \neq 0$$

when ψ has large enough conductor. So the number of χ with $L_p(1, \chi) = 0$ is bounded.

By the lemma,

$$\mathbb{Z}_p\text{-rank } \mathscr{X}_\infty/\omega_n\mathscr{X}_\infty = r_2 p^n + O(1).$$

By the structure theorem for $\mathscr{X}_\infty$, we see that the Λ-torsion contributes only bounded $\mathbb{Z}_p$-rank (at most λ) and $\Lambda^a/\omega_n\Lambda^a$ yields ap^n. Therefore we have proved the following.

Theorem 13.31. $\mathscr{X}_\infty \sim \Lambda^{r_2} \oplus (\Lambda\text{-}torsion)$. $\square$

One advantage of using $\mathscr{X}_\infty$ rather than X is that it is easier to describe how L_∞ is generated. Since all p-power roots of unity are in K_∞, M_∞/K_∞ is a Kummer extension. There is a subgroup

$$V \subseteq K_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

$$V = \{a \otimes p^{-n} \mid \text{various } n \ge 0 \text{ and } a \in K_\infty^\times\}$$

(it is not hard to see that all elements of $K_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are of the form $a \otimes p^{-n}$) such that

$$M_\infty = K_\infty(\{a^{1/p^n}\}).$$

There is a Kummer pairing

$$\mathscr{X}_\infty \times V \to W_{p^\infty} = p\text{-power roots of unity},$$

just as in Chapter 10. In particular,

$$(\sigma x, \sigma v) = (x, v)^\sigma, \qquad \sigma \in \mathrm{Gal}(K_\infty/F).$$

Let I_m be the group of fractional ideals of K_m and let $I_\infty = \bigcup I_m$. Since $a \otimes p^{-n}$ gives an extension unramified outside p, and since $a \in K_m$ for some m, it follows that

$$(a) = B_1^{p^n} \cdot B_2 \text{ in some } I_m,$$

know that

$$\mathrm{Gal}(M_n/K_0) \simeq \mathbb{Z}_p^{r_2 p^n + 1 + \delta_n} \times \text{(finite group)},$$

where $r_2 = r_2(K_0)$ and δ_n is the defect in Leopoldt's Conjecture (see Theorem 13.4). Therefore

$$\mathscr{X}_\infty/\omega_n \mathscr{X}_\infty \simeq \mathbb{Z}_p^{r_2 p^n + \delta_n} \times \text{(finite group)}.$$

By Lemma 13.16, $\mathscr{X}_\infty$ is a finitely generated Λ-module, so

$$\mathscr{X}_\infty \sim \Lambda^a \oplus (\Lambda\text{-torsion})$$

for some $a \geq 0$.

Lemma 13.30. *δ_n is bounded, independent of n.*

2nd edition correct proof

Proof. Suppose $\delta_n > 0$ for some n. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis for $E_1 = E_1(K_n)$ modulo roots of unity. We may assume $\varepsilon_{\delta_n+1}, \ldots, \varepsilon_r$ are independent over $\mathbb{Z}_p$ and generate $\bar{E}_1$ modulo torsion. Let $p^t = |(\bar{E}_1)_{\mathrm{tors}}|$. Then there exist $a_{ij} \in \mathbb{Z}_p$ such that

$$\varepsilon_i^{p^t} = \prod_{j > \delta_n} \varepsilon_j^{p^t a_{ij}} \qquad \text{for } 1 \leq i \leq \delta_n.$$

Let $m \geq t$ and let $a'_{ij} \in \mathbb{Z}$ satisfy $a'_{ij} \equiv a_{ij} \pmod{p^m}$. Let

$$\eta_i = \varepsilon_i \prod_j \varepsilon_j^{a'_{ij}} \qquad \text{for } 1 \leq i \leq \delta_n.$$

Then $\eta_i^{p^t}$ is a p^{m+t}th power in $\bar{E}_1 \subseteq \prod_{\wp|p} U_{1,\wp}$.

If $\eta \in K_n^\times$ is a pth power in $K_\infty^\times$, then $K_n(\eta^{1/p}) \subseteq K_\infty$. Since K_{n+1} is generated over K_n by a root of unity, η must be a p-th power times a root of unity in K_n.

Since $\varepsilon_1, \ldots, \varepsilon_{\delta_n}$ are independent in E_1, $\eta_1, \ldots, \eta_{\delta_n}$ generate a subgroup isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^{\delta_n}$ in $K_n^\times/(K_n^\times)^{p^m}$, hence in $K_\infty^\times/(K_\infty^\times)^{p^m}$ by the previous paragraph. Since $\zeta_p \in K_0$ by assumption, $\zeta_{p^n} \in K_\infty$ for all n. Therefore $K_\infty(\{\eta_i^{p^{t-m}}\})/K_\infty$ has Galois group $(\mathbb{Z}/p^{m-t}\mathbb{Z})^{\delta_n}$. Since each $\eta_i^{p^t}$ is a pth power locally at the primes dividing p, these primes split completely, hence do not ramify. Therefore the Galois group X of the maximal abelian unramified p-extension of K_∞ has a quotient isomorphic to $(\mathbb{Z}/p^{m-t}\mathbb{Z})^{\delta_n}$. In the decomposition of X, the terms of the form $\Lambda/(p^k)$ cannot account for this for large m. The term of the form $\bigoplus_j \Lambda/(g_j(T))$ can only yield $(\mathbb{Z}/p^{m-t}\mathbb{Z})^\lambda$, where $\lambda = \sum \deg g_j$. Therefore $\delta_n \leq \lambda$. This completes the proof. $\square$

If $\zeta_p \notin K_0$, the lemma is still true. Simply adjoin ζ_p and use the easily proved fact that if $K \subseteq L$ then $\delta(K) \leq \delta(L)$.

The above result perhaps could have been conjectured from Theorem 7.10 (although we already know $\delta_n = 0$ in that situation). Intuitively, the number δ_n should be approximately the number of occurrences of $L_p(1, \chi) = 0$ for K_n^+.