11. Eisenstein Reciprocity

In order to prove higher reciprocity laws, the methods known to Gauss were soon found to be inadequate. The most obvious obstacle, namely the fact that the unique factorization theorem fails to hold for the rings $\mathbb{Z}[\zeta_\ell]$, was overcome by Kummer through the invention of his ideal numbers. The direct generalization of the proofs for cubic and quartic reciprocity, however, did not yield the general reciprocity theorem for ℓ-th powers: indeed, the most general reciprocity law that could be proved within the cyclotomic framework is Eisenstein's reciprocity law. The key to its proof is the prime ideal factorization of Gauss sums; since we can express Gauss sums in terms of Jacobi sums and vice versa, the prime ideal factorization of Jacobi sums would do equally well.

Although Eisenstein's reciprocity law is only a very special case of more general reciprocity laws, it turned out to be an indispensable step for proving these general laws until Furtwängler [253] succeeded in finally giving a proof of the reciprocity law in $\mathbb{Q}(\zeta_\ell)$ without the help of Eisenstein's reciprocity law. It should also be noted that Eisenstein's reciprocity law holds for all primes ℓ, whereas Kummer had to assume that ℓ is regular, i.e. that ℓ does not divide the class number of $\mathbb{Q}(\zeta_\ell)$.

Using the prime ideal factorization of Gauss sums together with the trivial fact that the m^{th} power of Gauss sums generate principal ideals in $\mathbb{Z}[\zeta_m]$, we will be able to deduce amazing properties of ideal class groups of abelian extensions of $\mathbb{Q}$. This idea goes back to work of Jacobi, Cauchy and Kummer, was extended by Stickelberger and revived by Iwasawa. Later refinements and generalizations due to Thaine, Kolyvagin and Rubin will be discussed only marginally.

11.1 Factorization of Gauss Sums

In the mathematical literature there exist many proofs for the *Stickelberger relation*, which gives the prime ideal factorization of Gauss sums. The simplest proof unfortunately works only for the primes $p \equiv 1 \bmod m$, and this is why we treat this case separately.

First we will show that the Stickelberger relation follows almost from the fact that adjoining $G(\chi) = -\sum_{t\in\mathbb{F}_q^\times}\chi(t)\zeta_p^{\mathrm{Tr}\,(t)}$ to $\mathbb{Q}(\zeta_m)$ generates an abelian extension. We will complete the proof by following Hilbert's Zahlbericht [368].

Let $\mathfrak{p}$ be a prime ideal in $K = \mathbb{Q}(\zeta_m)$ above $p \equiv 1 \bmod m$, and suppose that χ is a multiplicative character of order m on $\mathbb{F} = \mathcal{O}_K/\mathfrak{p}$. From Chapter 4 we know that $G(\chi)^m \in \mathbb{Z}[\zeta_m]$; moreover, K is the decomposition field of $\mathfrak{p}$ in $L = \mathbb{Q}(\zeta_{pm})$, because $p \equiv 1 \bmod m$ guarantees that p splits completely in $K/\mathbb{Q}$. We also know from $G(\chi)\overline{G(\chi)} = p$ that only prime ideals above p can occur in the prime ideal factorization of $\mu = G(\chi)^m$. Since $\Gamma = \mathrm{Gal}\,(K/\mathbb{Q})$ acts transitively on the prime ideals above $\mathfrak{p}$, we can write $\mu\mathcal{O}_K = \mathfrak{p}^\gamma$ for some $\gamma = \sum_\sigma b_\sigma\sigma \in \mathbb{Z}[\Gamma]$, where $\mathbb{Z}[\Gamma]$ denotes the group ring of Γ, and where γ depends on the choice of the prime ideal $\mathfrak{p}$.

Remark. The group ring $\mathbb{Z}[G]$ of a finite group G is simply the set of formal sums $\{\sum_{\sigma\in G} a_\sigma\sigma\}$. If M is an abelian group on which G acts, then we can make $\mathbb{Z}[G]$ act on M via $\big(\sum_{\sigma\in G} a_\sigma\sigma\big)m = \sum_{\sigma\in G} a_\sigma\sigma(m)$. Actually, we have been doing this before without even noticing it when we used expressions like $\alpha^{\sigma-1}$ as an abbreviation for $\alpha^\sigma\alpha^{-1}$.

In order to determine γ we first take the absolute norm of μ^2 and find

$$\begin{aligned} N_{K/\mathbb{Q}}\mu^2 &= N_{K/\mathbb{Q}}(\mu\overline{\mu}) = N_{K/\mathbb{Q}}(p^m) = p^{m(K:\mathbb{Q})} = p^{m\phi(m)}, \text{ and} \\ N_{K/\mathbb{Q}}\mu &= N_{K/\mathbb{Q}}\mathfrak{p}^\gamma = p^S, \text{ where } S = \textstyle\sum_{\sigma\in\Gamma} b_\sigma. \end{aligned}$$

This implies $\sum_{\sigma\in\Gamma} b_\sigma = \frac{1}{2}m\phi(m)$. The proof we are about to give will proceed as follows:

1. First we observe that $0 \le b_\sigma \le m$: of course $b_\sigma \ge 0$ since $G(\chi)$ is integral; moreover, $b_\sigma \le m$ follows from $\mu\overline{\mu} = p^m$.
2. Then we will show that $(b_\sigma, m) = 1$; this will follow from the fact that adjoining $G(\chi)$ to K gives an extension L of degree $(L : K) = m$.
3. The fact that L/K is abelian will allow us to derive that the b_σ form a complete system of coprime residues mod m;
4. Finally, a simple inequality will imply that the b_σ take the minimal positive coprime residues mod m, and Stickelberger's relation will follow.

Now we will prove that $(a, m) = 1$, where $\mathfrak{p}^a \parallel \mu$. To this end we will show that $K(\sqrt[m]{\mu})/K$ is an abelian extension of degree m; once we know this, the proof of $(a, m) = 1$ is immediate: suppose that $b = (a, m)$; then $\mathfrak{p}$ has ramification index $\frac{m}{b}$ in $K(\sqrt[m]{\mu})/K$ by the decomposition law in Kummer extensions. On the other hand $K(\sqrt[m]{\mu})/K$ is a sub-extension of $K(\zeta_p)/K$, which is completely ramified above $\mathfrak{p}$: this shows that $\mathfrak{p}$ has ramification index $(K(\sqrt[m]{\mu}) : K) = m$. Comparing both expressions yields $b = 1$.

Lemma 11.1. *Let χ be a character of order m on $\mathbb{F}_p$, $p \equiv 1 \bmod m$, let $G(\chi)$ be the corresponding Gauss sum, and put $L = \mathbb{Q}(\zeta_m, G(\chi))$. Then $L \subseteq \mathbb{Q}(\zeta_{mp})$, and $(L : \mathbb{Q}(\zeta_m)) = m$.*

Proof. Let g be a primitive root mod p and put $k = L \cap \mathbb{Q}(\zeta_p)$; define $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_{mp})/\mathbb{Q})$ by $\sigma : \zeta_p \longmapsto \zeta_p^g, \ \ \zeta_m \longmapsto \zeta_m$. Now $\chi(g)$ is a primitive m-th root of unity, hence the relation $G(\chi)^\sigma = \chi(g)^{-1}G(\chi)$ shows that σ^m is the smallest power of σ fixing L. This shows that $L/\mathbb{Q}(\zeta_m)$ is cyclic of degree m, and our claim follows. □

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_{mp}) \arrow[dl, no head] \arrow[dr, no head] & \\
 & L \arrow[dl, no head] \arrow[dr, no head] & & \mathbb{Q}(\zeta_p) \arrow[dl, no head] \\
\mathbb{Q}(\zeta_m) \arrow[dr, no head] & & k \arrow[dl, no head] & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Now $L = K(\sqrt[m]{\mu})$ is an abelian extension of $\mathbb{Q}$; for each $\sigma \in \mathrm{Gal}\,(L/\mathbb{Q})$ define $a(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^\times$ by $\sigma(\zeta_m) = \zeta_m^{a(\sigma)}$. From Corollary 4.17 we infer that $\mu^{\sigma - a(\sigma)} = \xi^m$ for some $\xi \in L^\times$. This shows that the exponent of $\mathfrak{p}$ in $\mu^{\sigma-a(\sigma)}$ is divisible by m, i.e., that $\sigma\gamma \equiv a(\sigma)\gamma \bmod m$. Let σ_a denote the automorphism of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ mapping $\zeta_m \longmapsto \zeta_m^a$ and write $\gamma = \sum\limits_{(a,m)=1} b_a\sigma_a$. We find $\sigma_c\gamma = \sum b_a\sigma_a\sigma_c = \sum b_a\sigma_{ac}$ and $a(\sigma_c)\gamma = c\gamma = \sum a(\sigma)b_a\sigma_a = \sum a(\sigma)b_{ac}\sigma_{ac}$, hence $\sigma\gamma \equiv a(\sigma)\gamma \bmod m$ implies the congruence $b_{ac} \equiv c^{-1}b_a \bmod m$ for all $a, c \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Now choose t such that b_t is minimal among the b_c; then

$$\sum_a b_a = \sum_c b_{ct} \equiv \sum_c c^{-1}b_t = b_t \sum_c c^{-1} \bmod m.$$

On the other hand, letting $M \subset \{1, \ldots, m-1\}$ denote the set of minimal positive coprime residues mod m, we find

$$\sum_{c\in M} c = \frac{1}{2}\left(\sum_{c\in M} c + \sum_{c\in M}(m-c)\right) = \frac{1}{2}m\phi(m).$$

Since the b_a are integers ≥ 1, this shows that $\sum_a b_a = \frac{1}{2}m\phi(m)$ can only hold if $b_t = 1$, that is if the b_a actually take all the values of M exactly once. Therefore $G(\chi)^m\mathcal{O}_m = \mathfrak{p}^\gamma$ for some suitable prime ideal $\mathfrak{p}$ in $\mathcal{O}_m = \mathbb{Z}[\zeta_m]$ above p, with $\gamma = \sum_t t^{-1}\sigma_t \in \mathbb{Z}[\Gamma]$, and where t^{-1} denotes the smallest positive integer such that $t^{-1}t \equiv 1 \bmod m$. If we denote the fractional part of a real number x by $\langle x\rangle$ (i.e., $\langle x\rangle = x - \lfloor x\rfloor$, where $\lfloor\cdot\rfloor$ is Gauss's floor function), then $G(\chi)^m\mathcal{O}_m = \mathfrak{p}^\gamma$, $\gamma = m\theta$, with $\theta = \sum_{(t,m)=1}\langle\frac{t}{m}\rangle\sigma_t^{-1}$. We have seen

Proposition 11.2. *Let χ be a character of order m on $\mathbb{F}_p$, $p \equiv 1 \bmod m$, and let $G(\chi)$ be the corresponding Gauss sum. Then there exists a prime ideal $\mathfrak{p} \mid p\mathcal{O}_m$ such that*

$$G(\chi)^m\mathcal{O}_m = \mathfrak{p}^{m\theta}, \quad \theta = \sum_{\substack{0<t<m\\(t,m)=1}} \langle\tfrac{t}{m}\rangle\sigma_t^{-1}. \tag{11.1}$$

What we have proved so far about the prime ideal factorization of the Gauss sum would suffice to show that $\left(\frac{a}{\alpha}\right)_m = 1 \iff \left(\frac{\alpha}{a}\right)_m = 1$; if we want to prove that both expressions are always equal we need more information, i.e. we have to specify the prime ideal $\mathfrak{p}$ in the preceding proposition. In fact we claim that $\mathfrak{p} \parallel G(\chi)^m$ if $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$. Since $\mathfrak{p} = \mathfrak{P}^{p-1}$ in $\mathbb{Z}[\zeta_{mp}]$, we see that

$$\mathfrak{p} \parallel G(\chi)^m \iff \mathfrak{P}^{p-1} \parallel G(\chi)^m \iff \mathfrak{P}^{(p-1)/m} \parallel G(\chi).$$

Put $n = \frac{p-1}{m}$ and $\mathit{\Pi} = \zeta_p - 1$; we will compute $G(\chi) \bmod \mathit{\Pi}^{n+1}$:

Lemma 11.3. *Let the notation be as above. Then*

$$G(\chi) \equiv \frac{\mathit{\Pi}^n}{n!} \bmod \mathfrak{P}^{n+1}. \tag{11.2}$$

Proof. This is a slightly tricky computation:

$$\begin{aligned}
-G(\chi) = \quad & \sum_{a=1}^{p-1} \chi(a)\zeta_p^a \ = \sum_{a=1}^{p-1} \chi(a)(1+\mathit{\Pi})^a \ = \sum_{a=1}^{p-1} \chi(a) \sum_{j=0}^{a} \tbinom{a}{j} \mathit{\Pi}^j \\
\equiv^{1,2} & \sum_{j=0}^{n} \sum_{a=1}^{p-1} a^{p-1-n} \tbinom{a}{j} \mathit{\Pi}^j \ =^{3,4} \ \sum_{a=1}^{p-1} a^{p-1-n} \tbinom{a}{n} \mathit{\Pi}^n \\
= \quad & \sum_{a=1}^{p-1} a^{p-1-n} \frac{a^n}{n!} \mathit{\Pi}^n \ \equiv \ (p-1)\frac{\mathit{\Pi}^n}{n!} \ \equiv^5 \ -\frac{\mathit{\Pi}^n}{n!} \bmod \mathit{\Pi}^n \mathfrak{P}.
\end{aligned}$$

In this computation we have used the following facts:

1. $\chi(a) \equiv a^{p-1-n} \bmod \mathfrak{p}$;
2. $\mathit{\Pi}^j \equiv 0 \bmod \mathit{\Pi}^n$ for $j > n$;
3. $\binom{a}{j}$ is a polynomial of degree j in a; in particular, $a^{p-1-n}\binom{a}{j}$ contains a monomial of degree divisible by $p-1$ if and only if $j = n$;
4. $\sum_{a=1}^{p-1} a^k \equiv 0 \bmod p$ if k is not divisible by $p-1$ (see Proposition 4.29);
5. $\mathfrak{P} \mid \mathit{\Pi}$; in particular, the congruence $G(\chi) \equiv \mathit{\Pi}^n/n!$ is valid modulo $\mathfrak{P}^n$.

Observe the analogy to the computation in Section 8.7. □

The congruence $G(\chi) \equiv \mathit{\Pi}^n/n! \bmod \mathfrak{P}^{n+1}$ implies, as we already have pointed out, that $\mathfrak{p} \parallel G(\chi)^m$, and we have proved:

Theorem 11.4. *Let $p \equiv 1 \bmod m$ be prime, and let $\mathfrak{p}$ be a prime ideal above p in $K = \mathbb{Q}(\zeta_m)$. Then $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$ is a multiplicative character of order m on $\mathbb{F}_p$, and the corresponding Gauss sum $G(\chi)$ has the factorization $G(\chi)^m \mathcal{O}_m = \mathfrak{p}^{m\theta}$, where θ is defined in (11.1).*

This looks more complicated than it is; here are a few examples that illustrate the factorization of Gauss sums $G(\chi)^m$ for characters $\chi = (\cdot/\mathfrak{p})_m$ over $\mathbb{F}_p$, $p \equiv 1 \bmod m$; here $\mathfrak{p}_i$ denotes the prime ideal $\sigma_i(\mathfrak{p})$ with $\mathfrak{p} = \mathfrak{p}_1$:

m	$G(\chi^{-1})^m$	$G(\chi)^m$	$J(\chi,\chi)$
2	$\mathfrak p$	$\mathfrak p$	
3	$\mathfrak p_1\mathfrak p_2^2$	$\mathfrak p_1^2\mathfrak p_2$	$\mathfrak p_1$
4	$\mathfrak p_1\mathfrak p_3^3$	$\mathfrak p_1^3\mathfrak p_3$	$\mathfrak p_1$
5	$\mathfrak p_1\mathfrak p_2^3\mathfrak p_3^2\mathfrak p_4^4$	$\mathfrak p_1^4\mathfrak p_2^2\mathfrak p_3^3\mathfrak p_4$	$\mathfrak p_1\mathfrak p_3$
7	$\mathfrak p_1\mathfrak p_2^4\mathfrak p_3^5\mathfrak p_4^2\mathfrak p_5^3\mathfrak p_6^6$	$\mathfrak p_1^6\mathfrak p_2^3\mathfrak p_3^2\mathfrak p_4^5\mathfrak p_5^4\mathfrak p_6$	$\mathfrak p_1\mathfrak p_4\mathfrak p_5$
8	$\mathfrak p_1\mathfrak p_3^3\mathfrak p_5^5\mathfrak p_7^7$	$\mathfrak p_1^7\mathfrak p_3^5\mathfrak p_5^3\mathfrak p_7$	$\mathfrak p_1\mathfrak p_5$

The factorization of $G(\chi)^m$ into prime ideals follows from the factorization of $G(\chi^{-1})$ given Theorem 11.4 and the relation $G(\chi)G(\chi^{-1}) = \pm p$. The corresponding results for the Jacobi sum can be derived from $J(\chi,\chi)^m = G(\chi)^{2m}G(\chi^2)^{-m}$ and $G(\chi^2)^m = \sigma_2(G(\chi)^m)$ (the last equality only holds for odd m; if m is even, $G(\chi^2)$ is known from the computations for $m/2$).

For odd prime values of m, one finds (see Exercise 11.2)

Corollary 11.5. *Let ℓ and $p \equiv 1 \bmod \ell$ be odd primes; assume that $\mathfrak p$ is a prime ideal above p in $\mathbb Z[\zeta_\ell]$, and put $\chi = (\,\cdot\,/\mathfrak p)_\ell$. Then*

$$(J(\chi,\chi)) = \mathfrak p^s, \qquad s = \sum_{t=1}^{\ell-1} \left\lfloor \frac{2t}{\ell} \right\rfloor \sigma_{-t}^{-1}.$$

Turning this procedure around, one can prove Proposition 11.2 by exploiting the fact that Jacobi sums are integral (see Exercise 11.5).

11.2 Eisenstein Reciprocity for ℓ-th Powers

Now that we know the prime ideal factorization of the Gauss sum, we will use the special case $m = \ell$ prime to prove Eisenstein's reciprocity law. This law will take its simplest form if we restrict it to numbers $\equiv 1$ modulo a high power of $\lambda = 1 - \zeta_\ell$ (compare the special case of cubic and quartic residues). We will call $\alpha \in \mathbb Z[\zeta_\ell]$ *semi-primary* if $(\alpha,\ell) = 1$ and $\alpha \equiv a \bmod (1-\zeta_\ell)^2$ for some $a \in \mathbb Z$.

Lemma 11.6. *Let ℓ be an odd prime, and suppose that $(\alpha,\ell) = (\beta,\ell) = 1$ for some $\alpha,\beta \in \mathbb Z[\zeta_\ell]$. Then*

i) there is a unique $c \in \mathbb Z/\ell\mathbb Z$ such that $\zeta_\ell^c\alpha$ is semi-primary;
ii) if α,β are semi-primary, then so are $\alpha \pm \beta$ and $\alpha\beta$;
iii) α^ℓ is semi-primary;
iv) if $\alpha \in \mathbb Z[\zeta + \zeta^{-1}]$, then α is semi-primary;
v) if α is a semi-primary unit, then $\alpha \in \mathbb Z[\zeta + \zeta^{-1}]$;
vi) Jacobi sums are semi-primary; more exactly: if $\chi,\psi \neq 1\!\!1$ are characters of order ℓ on $\mathbb F_q$, then $J(\chi,\psi) \equiv 1 \bmod (1-\zeta_\ell)^2$.

Proof. These are straightforward computations: i) Let $\lambda = \zeta_\ell - 1$; then $\mathfrak{l} = (\lambda)$ is the prime ideal above ℓ in $\mathbb{Q}(\zeta_\ell)$, and we find

$$\alpha = \sum_{j=0}^{\ell-1} a_j \zeta_\ell^j = \sum_{j=0}^{\ell-1} a_j (1+\lambda)^j \equiv \sum_{j=0}^{\ell-1} a_j (1 + j\lambda) = a + b\lambda \bmod \mathfrak{l}^2$$

for some $a, b \in \mathbb{Z}$. Observe that $\ell \nmid a$ since $(\alpha, \ell) = 1$, and define $c \in \mathbb{Z}$ by $ac \equiv b \bmod \ell$; then $\zeta_\ell^c = (1-\lambda)^c \equiv 1 - c\lambda \bmod \mathfrak{l}^2$, hence $\zeta_\ell^c \alpha \equiv (a + b\lambda)(1 - c\lambda) \equiv a + (ac - b)\lambda \equiv a \bmod \mathfrak{l}^2$.
ii) is clear;
iii) Let $\alpha \equiv \beta \bmod \lambda$; then $\alpha^\ell - \beta^\ell = \prod_{j=0}^{\ell-1}(\alpha - \zeta^j \beta) \equiv 0 \bmod \lambda^\ell$. Thus $\alpha \equiv a \bmod \lambda$ implies immediately $\alpha^\ell \equiv a^\ell \equiv a \bmod (1-\zeta)^2$, and α^ℓ is semi-primary as claimed.
iv) Assume that $\alpha \equiv a + b\lambda \bmod \lambda^2$ for integers $a, b \in \mathbb{Z}$; then $\alpha \equiv a + b - b\zeta \bmod \lambda^2$ and $\overline{\alpha} \equiv a + b - b\zeta^{-1} \bmod \lambda^2$ imply that $0 = \alpha - \overline{\alpha} \equiv b(\zeta - \zeta^{-1}) \bmod \lambda^2$, since α is real. But $\lambda \,\|\, (\zeta - \zeta^{-1})$ shows $b \equiv 0 \bmod \lambda$, hence we have $b \equiv 0 \bmod \ell$ and $\alpha \equiv a \bmod \lambda^2$.
v) We can write $\alpha = \pm\zeta^j \alpha_0$, where $\alpha_0 \in \mathbb{Z}[\zeta + \zeta^{-1}]$ is a real unit. Since α is semi-primary, we have $\alpha \equiv a \bmod \lambda^2$. Now $a \equiv \overline{\alpha} \equiv \pm\zeta^{-j}\alpha_0 \bmod \lambda^2$, together with the fact that $\lambda \nmid \alpha_0$ (since α_0 is a unit) implies $\lambda^2 \mid (\zeta^j - \zeta^{-j})$; this in turn is only possible if $j \equiv 0 \bmod \ell$, i.e., if $\alpha = \alpha_0$ is real.
vi) using the congruences $(\chi(t) - 1)\psi(1-t) \equiv \chi(t) - 1 \bmod (1-\zeta_\ell)^2$ and $q \equiv p^f \equiv 1 \bmod \ell$ we find

$$\begin{aligned} J(\chi, \psi) &= -\textstyle\sum_{t \neq 0,1} \chi(t)\psi(1-t) \\ &= -\textstyle\sum_{t \neq 0,1} (\chi(t) - 1)\psi(1-t) - \sum_{t \neq 0,1} \psi(1-t) \\ &\equiv -\textstyle\sum_{t \neq 0,1} (\chi(t) - 1) - \sum_{t \neq 0,1} \psi(1-t) \\ &\equiv \chi(1) + \psi(1) + (q - 2) = q \equiv 1 \bmod (1-\zeta_\ell)^2. \end{aligned}$$

This completes the proof. □

Our next result concerns the power character of $\mu = G(\chi)^m$; since the proof does not depend on $m = \ell$ being prime, we treat the general case of arbitrary $m \geq 2$ (observe that the lemma below contains the quadratic reciprocity law as the special case $m = 2$!):

Lemma 11.7. *Let $p \equiv 1 \bmod m$ be prime, let $\mathfrak{p}$ be a prime ideal above p in $K = \mathbb{Q}(\zeta_m)$, and let $\mu = G(\chi)^m$, where $G(\chi)$ is the Gauss sum corresponding to $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)^{-1}$. Then for all prime ideals $\mathfrak{q}$ in $\mathcal{O}_k$ such that $\mathfrak{q} \nmid pm$ we have*

$$\left(\frac{\mu}{\mathfrak{q}}\right)_m = \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m,$$

where $N\mathfrak{q} = q^f$ is the absolute norm of $\mathfrak{q}$.

Proof. The decomposition law in cyclotomic fields implies the congruence $q^f \equiv 1 \bmod m$; hence

$$\begin{aligned}(-G(\chi))^{q^f} &\equiv \textstyle\sum_t \chi(t)^{q^f} \zeta_m^{tq^f} \;=\; \sum_t \chi(t)\zeta_m^{tq^f} \\ &= -\chi(q^f)^{-1} G(\chi) \;=\; \left(\tfrac{N\mathfrak{q}}{\mathfrak{p}}\right)_m (-G(\chi)) \bmod q\mathcal{O}_k .\end{aligned}$$

This implies $(-G(\chi))^{q^f-1} \equiv \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m \bmod q$. On the other hand we have

$$(-G(\chi))^{q^f-1} = ((-1)^m \mu)^{(q^f-1)/m} \equiv \left(\frac{\mu}{\mathfrak{q}}\right)_m \bmod \mathfrak{q},$$

and comparing both expressions we get the claimed equality. □

For each prime ideal $\mathfrak{p} \nmid m$ in $\mathbb{Z}[\zeta_m]$ define $\Phi(\mathfrak{p}) = G(\chi_{\mathfrak{p}})^m$ with $\chi_{\mathfrak{p}} = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$; we extend Φ multiplicatively to all ideals prime to m, and from the multiplicativity of Φ, the norm N, and of the power residue symbol $\left(\frac{\cdot}{\cdot}\right)_m$ we deduce that

$$\left(\frac{\Phi(\mathfrak{a})}{\mathfrak{q}}\right)_m = \left(\frac{N\mathfrak{q}}{\mathfrak{a}}\right)_m \tag{11.3}$$

for all ideals $\mathfrak{a}$ which are products of prime ideals of degree 1 not dividing m. Observe that we did not use the Stickelberger relation for deriving (11.3). It comes in now: if $\mathfrak{a} = \alpha\mathcal{O}_k$ is principal, then there exists a unit $\varepsilon(\alpha) \in \mathcal{O}_k^\times$ such that

$$\Phi(\mathfrak{a}) = \varepsilon(\alpha)\alpha^\gamma, \tag{11.4}$$

where $\gamma = m\theta \in \mathbb{Z}[G]$ as in (11.1). We want to compute the residue symbol $(\alpha^\gamma/\mathfrak{q})$: first note that, for $m = \ell$ prime,

$$\left(\frac{\sigma_t^{-1}(\alpha^t)}{\mathfrak{q}}\right)_\ell = \left(\frac{\sigma_t^{-1}(\alpha)}{\mathfrak{q}}\right)_\ell^t = \left(\frac{\sigma_t^{-1}(\alpha)}{\mathfrak{q}}\right)_\ell^{\sigma_t} = \left(\frac{\alpha}{\mathfrak{q}^{\sigma_t}}\right)_\ell ;$$

this shows immediately that

$$\left(\frac{\alpha^\gamma}{\mathfrak{q}}\right)_\ell = \prod_t \left(\frac{\alpha}{\mathfrak{q}^{\sigma_t}}\right)_\ell = \left(\frac{\alpha}{N\mathfrak{q}}\right)_\ell ,$$

where $N\mathfrak{q} = p^f$ denotes the absolute norm of $\mathfrak{q}$. Since we have proved Stickelberger's relation only for prime ideals of degree 1, the reciprocity formula just proved is only valid for such α which are products of prime ideals of degree 1. Before we will see how Hilbert dealt with this difficulty, we take care of the unit $\varepsilon(\alpha)$ defined in Equation (11.4): if we want a simple formula like $\left(\frac{\alpha}{N\mathfrak{q}}\right)_\ell = \left(\frac{N\mathfrak{q}}{\alpha}\right)_\ell$ to hold, we must make sure that $\varepsilon(\alpha)$ is an ℓ-th power residue modulo all prime ideals $\mathfrak{q}$: the only way to do this is to show that $\varepsilon(\alpha)$ is an actual ℓ-th power if α is semi-primary:

Lemma 11.8. *The unit $\varepsilon(\alpha)$ defined in Equation (11.4) is a root of unity, and if α is semi-primary and $m = \ell$ is an odd prime, then $\varepsilon(\alpha) = \pm 1$.*

Proof. We begin by showing that $\varepsilon(\alpha)$ is an m-th root of unity. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is abelian it is sufficient to show that $|\,\varepsilon(\alpha)\,| = 1$, because this implies that $|\,\varepsilon(\alpha)^\sigma\,| = 1$ for all $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and a well known result due to Kronecker asserts that the only algebraic integers with this property are roots of unity.

The fact that $|\,\Phi(\mathfrak{p})\,|^2 = p = N\mathfrak{p}$ for all prime ideals of degree 1 implies at once that $|\,\Phi(\alpha)\,|^2 = |\,N(\alpha)\,|^m$. On the other hand, letting $\sigma = \sigma_{-1}$ denote complex conjugation we have $|\,\alpha^\gamma\,|^2 = \alpha^\gamma \alpha^{\gamma\sigma}$ and

$$\begin{aligned}\gamma(1+\sigma) &= \textstyle\sum t^{-1}\sigma_t + \sum t^{-1}\sigma_t\sigma_{-1} = \sum t^{-1}\sigma_t + \sum t^{-1}\sigma_{-t} \\ &= \textstyle\sum t^{-1}\sigma_t + \sum (m-t)^{-1}\sigma_t = m\sum \sigma_t,\end{aligned}$$

hence $\alpha^\gamma\alpha^{\gamma\sigma} = |\,N(\alpha)\,|^m$. This yields our first claim that $|\,\varepsilon(\alpha)\,| = 1$.

This much is true without m being prime or α being semi-primary – now we suppose that $\alpha \equiv z \bmod \mathfrak{l}^2$, where $\mathfrak{l} = (1-\zeta_\ell)\mathcal{O}_k$ is the prime ideal above the rational prime $m = \ell$. Applying $\sigma \in \mathrm{Gal}\,(k/\mathbb{Q})$ yields $\alpha^\sigma \equiv z \bmod \ell^2$, since ℓ is an ambiguous ideal, i.e. $\ell^\sigma = \ell$. This shows that

$$\alpha^\gamma \equiv z^\gamma \equiv z^{1+2+\ldots+(\ell-1)} \equiv z^{\ell(\ell-1)/2} \equiv \Big(\frac{z}{\ell}\Big)^\ell \equiv \pm 1 \bmod \mathfrak{l}^2.$$

Now look at $\Phi(\alpha) = \varepsilon(\alpha)\alpha^\gamma$: if we can show that $\Phi(\alpha) \equiv \pm 1 \bmod \mathfrak{l}^2$, then we can conclude that, for semi-primary α, we have $\varepsilon(\alpha) \equiv \pm 1 \bmod \mathfrak{l}^2$. But the only semi-primary roots of unity are ± 1, and this proves our claim.

The proof of the congruence $\Phi(\alpha) \equiv 1 \bmod \mathfrak{l}^2$ is straightforward:

$$\Phi(\alpha) = G(\chi_\mathfrak{p})^\ell = \Big(-\sum_{t\neq 0}\chi_\mathfrak{p}(t)\psi(t)\Big)^\ell \equiv -\sum_{t \neq 0}\psi(\ell t) = \psi(0) = 1 \bmod \ell,$$

and this suffices because $\mathfrak{l}^2 \mid \ell$ for $\ell > 2$. □

Now we will remove the condition that (α) be a product of prime ideals of degree 1. To this end let $\alpha \in \mathcal{O}_k$ be a semi-primary integer, assume that $\sigma : \zeta_\ell \longmapsto \zeta_\ell^r$ generates $\mathrm{Gal}\,(k/\mathbb{Q})$, and define

$$\beta = \alpha^S, \quad \text{where } S = \prod(1-\sigma^e);$$

here the product is over all integers $e \neq \ell - 1$ which divide $\ell - 1$. We claim that only prime ideals of degree 1 occur in the prime ideal factorization of $\beta\mathcal{O}_k$. In fact, suppose that $\mathfrak{p}$ is a prime ideal of degree $f > 1$ dividing β. Put $ef = \ell - 1$: then $(1-\sigma^e)$ occurs in the product S above, and we can write $\beta = (\alpha^{h(\sigma)})^{1-\sigma^e}$, where h is some polynomial in $\mathbb{Z}[x]$. But σ^e fixes $\mathfrak{p}$, hence $\mathfrak{p}$ divides the numerator and the denominator of β equally often, and this shows that it cannot occur in the prime ideal factorization of $\beta\mathcal{O}_k$.

Since α is semi-primary, so is β, and from what we have proved we know that $(\beta/q) = (q/\beta)$. We also know that $(\alpha^\sigma/q)_\ell = (\alpha/q)_\ell^\sigma = (\alpha/q)_\ell^r$, hence we find

$$\begin{aligned} \Big(\frac{\alpha}{q}\Big)_\ell^{\prod(1-r^e)} &= \Big(\frac{\alpha}{q}\Big)_\ell^{\prod(1-\sigma^e)} = \Big(\frac{\beta}{q}\Big)_\ell = \Big(\frac{q}{\beta}\Big)_\ell \\ &= \Big(\frac{q}{\alpha}\Big)_\ell^{\prod(1-\sigma^e)} = \Big(\frac{q}{\alpha}\Big)_\ell^{\prod(1-r^e)}. \end{aligned}$$

But since the product of the numbers $1-r^e$ is not divisible by ℓ, we conclude that $(\alpha/q) = (q/\alpha)$. At this point we know that $(\alpha/q)_\ell = (q/\alpha)_\ell$ holds for all semi-primary $\alpha \in \mathcal{O}_k$ and all primes $q \neq \ell$. Since $(\cdot/\cdot)_\ell$ is multiplicative in the denominator, we have proved $(\alpha/a)_\ell = (a/\alpha)_\ell$ for all semi-primary $\alpha \in \mathcal{O}_k$ and all $a \in \mathbb{Z}$ not divisible by ℓ.

Theorem 11.9. (Eisenstein's Reciprocity Law for ℓ-th Powers) *Let $\ell \in \mathbb{N}$ be prime and suppose that $a \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[\zeta_\ell]$ are relatively prime and semi-primary; then*

$$\Big(\frac{a}{\alpha}\Big)_\ell = \Big(\frac{\alpha}{a}\Big)_\ell.$$

Moreover, we have

i) $\big(\frac{\alpha}{a}\big) = 1$ if $(\alpha, a) = 1$ and $\alpha \in \mathbb{Z}[\zeta_\ell + \zeta_\ell^{-1}]$ is real;
ii) $\big(\frac{a}{b}\big) = 1$ for all $a, b \in \mathbb{Z}$ such that $(a, b) = (b, \ell) = 1$.
iii) The first supplementary law: $\big(\frac{\zeta}{a}\big) = \zeta^{(a^{\ell-1}-1)/\ell}$.
iv) The second supplementary law: $\big(\frac{1-\zeta}{a}\big) = \big(\frac{\zeta}{a}\big)^{\frac{\ell-1}{2}}$.

Proof. Only the assertions i) – iv) are left to prove:
i) Let $G = \mathrm{Gal}\,(k/\mathbb{Q})$ denote the Galois group of $k = \mathbb{Q}(\zeta_\ell)$; then complex conjugation τ generates a subgroup $H = \langle\tau\rangle$ of order 2 in G. For a prime p let $\mathfrak{p}$ denote a prime ideal in $\mathcal{O}_k$ above p. Then

$$\Big(\frac{\alpha}{\mathfrak{p}^\tau}\Big) = \Big(\frac{\alpha^\tau}{\mathfrak{p}^\tau}\Big) = \Big(\frac{\alpha}{\mathfrak{p}}\Big)^\tau = \Big(\frac{\alpha}{\mathfrak{p}}\Big)^{-1}$$

implies that

$$\Big(\frac{\alpha}{p}\Big) = \prod_{\sigma \in G/H} \Big(\frac{\alpha}{\mathfrak{p}^\sigma \mathfrak{p}^{\sigma\tau}}\Big) = 1.$$

ii) If $\ell \nmid a$ this is a special case of i); but now $\big(\frac{\ell}{b}\big) = \big(\frac{\ell-b}{b}\big) = 1$.
iii) Let $p\mathcal{O}_k = \mathfrak{p}_1 \ldots \mathfrak{p}_g$; then

$$\Big(\frac{\zeta}{p}\Big) = \prod_{j=1}^{g} \Big(\frac{\zeta}{\mathfrak{p}_j}\Big) = \prod_{j=1}^{g} \zeta^{\frac{p^f-1}{\ell}} = \zeta^{g\,\frac{p^f-1}{\ell}}.$$

The observation

$$\frac{p^{fg}-1}{\ell} = \frac{p^f-1}{\ell}\cdot\left(p^{f(g-1)}+\ldots+p^f+1\right) \equiv g\cdot\frac{p^f-1}{\ell} \bmod \ell$$

shows that the claim holds for prime $a = p$. Now

$$\begin{aligned}\frac{(mn)^{\ell-1}-1}{\ell} &= \frac{m^{\ell-1}-1}{\ell}n^{\ell-1} + \frac{n^{\ell-1}-1}{\ell}\\ &\equiv \frac{m^{\ell-1}-1}{\ell} + \frac{n^{\ell-1}-1}{\ell} \quad \bmod \ell\end{aligned}$$

proves the assertion by induction on the primes dividing a.
iv) This follows immediately from i), iii), and the fact that $(1-\zeta)^2\zeta^{-1}$ is real. □

11.3 The Stickelberger Congruence

If p is a prime which does not split completely in $\mathbb{Q}(\zeta_m)$, then the computation of the prime ideal factorization of the Gauss sum corresponding to a character on $\mathbb{Z}[\zeta_m]/\mathfrak{p} \simeq \mathbb{F}_{p^f}$ becomes more difficult: historically, the first obstacle was overcome by Galois through his construction of finite fields; the first character sums over finite fields of order p^2 and p^3 were studied by Eisenstein [Eis], Kummer [465, §2] gave the prime ideal factorization of Jacobi sums in the general case, and Stickelberger [759] gave the corresponding result for Gauss sums that will be discussed below. The main idea will be to study the prime ideal decomposition of Gauss sums for characters χ over $\mathbb{F}_q$ first in the field $\mathbb{Q}(\zeta_{p(q-1)})$, and then take norms down to $\mathbb{Q}(\zeta_m)$, where m is the order of χ.

We start by introducing some notation. Let $q = p^f$ be the power of a prime p which will remain fixed throughout this section. For an integer $a \in \mathbb{Z}$, let $\overline{a}$ denote the unique integer satisfying $0 \le \overline{a} < q-1$ and $a \equiv \overline{a} \bmod q-1$. Write it in the form

$$\overline{a} = a_0 + a_1 p + \ldots + a_{f-1}p^{f-1}. \tag{11.5}$$

Then we define $s(a) = a_0 + a_1 + \ldots + a_{f-1}$ and $\gamma(a) = a_0!a_1!\cdots a_{f-1}!$.

Theorem 11.10. *Let $\mathfrak{P}$ be a prime ideal above p in $\mathbb{Q}(\zeta_{q-1})$, and let $\omega = (\,\cdot\,/\mathfrak{P})^{-1}$. Then the corresponding Gauss sums $G(\omega^a)$ satisfy the Stickelberger congruence*

$$\frac{G(\omega^a)}{\pi^{s(a)}} \equiv \frac{1}{\gamma(a)} \bmod \mathcal{P} \tag{11.6}$$

for all $a \in \mathbb{N}$, where $\pi = \zeta_p - 1$ and $\mathcal{P} = (\mathfrak{P}, \pi)$. Since $\mathcal{P} \parallel \pi$ and $\gamma(a)$ is a $\mathcal{P}$-adic unit, this implies in particular that $\mathcal{P}^{s(a)} \parallel G(\omega^a)$.

This is the main theorem on Gauss sums – among its corollaries are Theorems 4.31 and 4.32 of Davenport-Hasse (see [DaH] and Exercise 11.9) as well as a host of amazing results on class groups of abelian extensions of $\mathbb{Q}$, some of which we will discuss below. Also note that the choice $a = \frac{p-1}{2}$ turns (11.6) into (8.35), since $\omega^{(p-1)/2} = (\frac{\cdot}{p})$ is the quadratic residue character. The Hasse diagram for the fields and ideals occurring in the proofs below are displayed in Figure 11.1.

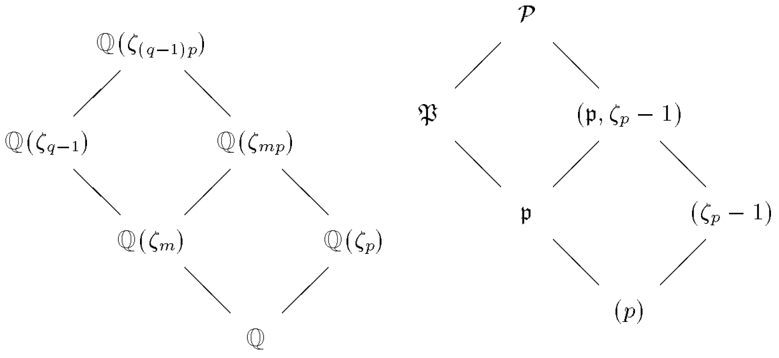

Fig. 11.1. Some subfields of $\mathbb{Q}(\zeta_{(q-1)p})$

Proof of Theorem 11.10. We will prove Stickelberger's congruence by induction on $s(a)$. For $s(a) = 0$, the claim is trivial (recall that $G(\mathbb{1}) = 1$). If $s(a) = 1$, then $a = p^r$ for some $r \geq 1$. Now

$$G(\omega^p) = G(\omega), \quad s(ap) = s(a) \quad \text{and} \quad \gamma(ap) = \gamma(a). \tag{11.7}$$

The last two equations are obvious, and the first is proved easily: since $G(\omega^p) = -\sum_{t \in \mathbb{F}_q^\times} \chi(t^p)\zeta^{\mathrm{Tr}\,(t)}$, it is sufficient to prove that $\mathrm{Tr}\,(t) = \mathrm{Tr}\,(t^p)$. But this is clear in light of $\mathrm{Tr}\,(t) = t + t^p + \ldots + t^{p^{f-1}}$.

Therefore it is sufficient to prove the claim for $a = 1$. This is done as follows: first we notice that

$$-G(\omega) = \sum_{t \in \mathbb{F}_q^\times} \omega(t)\zeta^{\mathrm{Tr}\,(t)} = \sum_{t \in \mathbb{F}_q^\times} \omega(t)(\zeta^{\mathrm{Tr}\,(t)} - 1)$$

since $\sum_t \omega(t) = 0$. The last sum has the advantage that all summands are divisible by $\zeta - 1$; moreover,

$$\frac{\zeta^m - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \ldots + \zeta^{m-1} \equiv m \bmod \pi$$

since $\zeta^r \equiv 1 \bmod \pi$ for all $r \in \mathbb{Z}$. This shows $-\frac{G(\omega)}{\pi} \equiv \sum_t \omega(t)\mathrm{Tr}\,(t) \bmod \pi$. Since we are summing over roots of unity t, we have $\omega(t) = t^{-1}$ and $\mathrm{Tr}\,(t) = t + t^p + \ldots + t^{p^{f-1}}$. Thus

$$\begin{aligned} -\frac{G(\omega)}{\pi} &\equiv \sum_{t \in \mathbb{F}_q^\times} t^{-1}\big(t + t^p + \ldots + t^{p^{f-1}}\big) \\ &= \sum_{t \in \mathbb{F}_q^\times} \big(1 + t + \ldots + t^{p^{f-2}}\big) = (q-1) \equiv -1 \bmod \mathcal{P}. \end{aligned}$$

This proves Stickelberger's congruence for $a = 1$, thus for all $a < q - 1$ such that $s(a) = 1$.

Now we do the induction step, so assume that (11.6) is proved for all $0 < a < q - 1$ with $s(a) \le r$, $r \ge 1$. Suppose $s(a) = r + 1$ and write $a = a_ip^i + \ldots a_{f-1}p^{f-1}$ with $a_i > 0$. Using (11.7) we may assume that $i = 0$, i.e. that $a = a_0 + a_1p + \ldots a_{f-1}p^{f-1}$ with $a_0 > 0$. Then $a - 1 = a_0 - 1 + a_1p + \ldots a_{f-1}p^{f-1}$, hence $s(a-1) = s(a) - 1$, and

$$\frac{G(\omega^{a-1})}{\pi^{s(a-1)}} \equiv \frac{1}{\gamma(a-1)} \bmod \mathcal{P}$$

from the induction assumption. Next $G(\omega^{a-1})G(\omega) = G(\omega^a)J(\omega, \omega^{a-1})$, and writing $b = q - 1 - (a-1) = q - a$ we find

$$\begin{aligned} -J(\omega, \omega^{a-1}) &\equiv \sum_t t^{-1}(1-t)^b \equiv \sum_t t^{-1} \sum_{j=0}^{b} (-1)^j \binom{b}{j} t^j \\ &= \sum_{j=0}^{q-1} (-1)^j \binom{b}{j} \sum_t t^{j-1} \bmod \mathfrak{P}. \end{aligned}$$

Since the inner sum vanishes modulo $\mathfrak{p}$ unless $j - 1$ is divisible by $q - 1$ (which happens if and only if $j = 1$), we get

$$J(\omega, \omega^{a-1}) \equiv -\tbinom{b}{1} = -b = a - q \equiv a \equiv a_0 \bmod \mathfrak{P}.$$

In particular, $J(\omega, \omega^{a-1})$ is a $\mathfrak{P}$-unit, and we conclude that

$$\frac{G(\omega^a)}{\pi^{s(a)}} = \frac{G(\omega^{a-1})}{\pi^{s(a-1)}}\frac{G(\omega)}{\pi^{s(1)}} J(\omega, \omega^{a-1})^{-1} \equiv \frac{1}{\gamma(a-1)}\frac{1}{a_0} = \frac{1}{\gamma(a)} \bmod \mathcal{P}.$$

This proves our claims. □

Since $\gamma(a)$ is a $\mathcal{P}$-adic unit and $\mathcal{P} \parallel \pi$, the Stickelberger congruence implies that $\mathcal{P}^{s(a)} \parallel G(\omega^a)$. In order to find the complete prime ideal factorization of $G(\omega^a)$, let $\sigma_b \in \Gamma = \mathrm{Gal}\,(\mathbb{Q}(\zeta_{p(q-1)})/\mathbb{Q})$ be defined by $\sigma_b : \zeta_{q-1} \longmapsto \zeta_{q-1}^b$, $\zeta_p \longmapsto \zeta_p$. Assume that $\mathcal{P}^{r\sigma_b^{-1}} \parallel G(\omega^a)$; applying σ_b gives $\mathcal{P}^r \parallel G(\omega^a)^{\sigma_b} = G(\omega^{ab})$, and we see that $r = s(ab)$.

Corollary 11.11. *We have* $(G(\omega^a)) = \mathcal{P}^{\Theta}$, *where* $\Theta = \sum_{\sigma_b \in \Gamma/Z} s(ab)\sigma_b^{-1}$. *Here* Z *denotes the decomposition group of* p.

This corollary gives the complete prime ideal factorization of Gauss sums; we will now show that the formulation of Theorem 11.4 carries over to the general case:

Theorem 11.12. *Let* $p \nmid m$ *be prime and let* $\mathfrak{p}$ *be a prime ideal above* p *in* $K = \mathbb{Q}(\zeta_m)$; *then* $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$ *is a multiplicative character of order* m *on* $\mathbb{F} = \mathbb{F}_q$, *where* $q = p^f = N\mathfrak{p}$ *is the absolute norm of* $\mathfrak{p}$. *The corresponding Gauss sum* $G(\chi) = -\sum_{t \in \mathbb{F}^\times} \chi(t)\zeta_m^{Tr(t)}$ *has the factorization* $G(\chi)^m = \mathfrak{p}^{m\theta}$ *for* θ *as in (11.1).*

Proof. We start by recalling that the decomposition group Z of $\mathcal{P}$ is generated by σ_p (see Proposition 3.1.iv), hence we have $Z = \{1, \sigma_p, \ldots, \sigma_p^{p^{f-1}}\}$. Now we need

$$s(a) = (p-1)\sum_{i=0}^{f-1}\Big\langle \frac{ap^i}{q-1}\Big\rangle. \tag{11.8}$$

For a proof, consider the following set of congruences modulo $q-1$:

$$\begin{array}{lllll} a & = a_0 & + a_1 p + \ldots + a_{f-1}p^{f-1} & \\ ap & \equiv a_{f-1} & + a_0 p + \ldots + a_{f-2}p^{f-1} & \bmod (q-1) \\ & \ldots & & \\ ap^{f-1} & \equiv a_1 & + a_2 p + \ldots + a_0 p^{f-1} & \bmod (q-1) \end{array}$$

The right hand side of the i-th congruence equals $(q-1)\langle \frac{ap^{i-1}}{q-1}\rangle$; summing up we find

$$\sum_{i=0}^{f-1}\Big\langle \frac{ap^i}{q-1}\Big\rangle = s(a)\frac{1+p+\ldots+p^{f-1}}{q-1} = \frac{s(a)}{p-1},$$

and this proves (11.8). Using (11.8) we get

$$s(ab)\sigma_b^{-1} = (p-1)\sum_{i=0}^{f-1}\Big\langle \frac{abp^i}{q-1}\sigma_b^{-1}\Big\rangle \equiv (p-1)\sum_{i=0}^{f-1}\Big\langle \frac{abp^i}{q-1}\sigma_{bp^i}^{-1}\Big\rangle \bmod Z,$$

hence

$$\sum_{\sigma_b \in \Gamma/Z} s(ab)\sigma_b^{-1} \equiv (p-1)\sum_{t \bmod q-1}\Big\langle \frac{at}{q-1}\Big\rangle \sigma_t^{-1} \bmod Z.$$

Using $\mathcal{P}^{p-1} = \mathfrak{P}$, we find

$$(G(\omega^a)) = \mathfrak{P}^T, \quad \text{where } T = \sum_{t \bmod q-1} \Big\langle \frac{at}{q-1} \Big\rangle \sigma_t^{-1}. \tag{11.9}$$

Now we are in a position to complete the proof by using Kummer's trick (cf. Section 10.2) of going up to $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$, where $q = p^f = N\mathfrak{p}$: every ideal prime to m in $\mathbb{Z}[\zeta_m]$ has norm $\equiv 1 \bmod m$, hence, in particular, $q \equiv 1 \bmod m$. Let $\mathfrak{P}$ denote the prime ideal above $\mathfrak{p}$ in $\mathbb{Q}(\zeta_{q-1})$; then $\mathfrak{P}$ still has inertia degree f, hence $\mathcal{O}_{q-1}/\mathfrak{P} \simeq \mathcal{O}_m/\mathfrak{p} \simeq \mathbb{F}_q$. The advantage of working in $\mathcal{O}_{q-1}$ is, as we have seen, that $(\mathcal{O}_{q-1}/\mathfrak{P})^\times$ has μ_{q-1} as a set of representatives.

We have $\chi = \omega^a$ with $a = \frac{q-1}{m}$. From (11.9) we get

$$G(\chi) = \mathfrak{P}^T, \quad \text{with } T = \sum_{t \bmod q-1} \Big\langle \frac{t}{m} \Big\rangle \sigma_t^{-1}. \tag{11.10}$$

Next let us look at the automorphisms of $\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m)$. Write $q-1 = mn$; then $\sigma_t : \zeta_{q-1} \longmapsto \zeta_{q-1}^t$ fixes $\zeta_m = \zeta_{q-1}^n$ if and only if $nt \equiv 1 \bmod q-1$, i.e. if and only if $t \equiv 1 \bmod m$. We conclude that the relative norm of $\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m)$ is simply $\nu = \sigma_1 + \sigma_{1+m} + \ldots + \sigma_{1+m(n-1)}$. Since $\langle \frac{t}{m} \rangle$ in (11.10) only depends on $t \bmod m$, we can write

$$\begin{aligned}\sum_{t \bmod q-1} \Big\langle \frac{t}{m} \Big\rangle \sigma_t^{-1} &= \sum_{t \bmod m} \Big\langle \frac{t}{m} \Big\rangle \sum_{j=0}^{n-1} \sigma_{t+jm}^{-1} \\ &= \sum_{j=0}^{n-1} \sigma_{1+jm} \sum_{t \bmod m} \Big\langle \frac{t}{m} \Big\rangle \sigma_t^{-1}\end{aligned}$$

Since the first sum is just the relative norm ν that occurred before, we find, using $\mathfrak{P}^\nu = \mathfrak{p}$, that

$$G(\chi)^m = \mathfrak{p}^{m\theta}, \quad \text{with } \theta = \sum_{(t,m)=1} \langle \tfrac{t}{m} \rangle \sigma_t^{-1}. \tag{11.11}$$

This concludes our proof. □

Congruences for Jacobi Sums

Equation (11.6) also generalizes many of the congruences for cubic and quartic Jacobi sums that we have proved. In fact, assume for the sake of simplicity that $f = 1$, that is, let $p = mn + 1$ be prime, $K = \mathbb{Q}(\zeta_m)$, let $\mathfrak{p}$ denote a prime ideal in $\mathcal{O}_K$ above p, and let $\chi = (\,\cdot\,/\mathfrak{p})_m^{-1}$. Then $s(a) = a$ for $0 < a < m$, and we can identify χ with $\omega^{(p-1)/m} = \omega^n$ via the isomorphism $(\mathcal{O}_K/\mathfrak{p})^\times \simeq (\mathbb{Z}[\zeta_{p(q-1)}]/\mathcal{P})^\times$. Now Stickelberger's congruence gives $G(\chi^a)/\pi^a \equiv 1/(an)! \bmod \mathcal{P}$. This implies

$$J(\chi^a, \chi^b) \;=\; \frac{G(\chi^a)G(\chi^b)}{G(\chi^{a+b})} \;\equiv\; \frac{(an+bn)!}{(an)!\,(bn)!} = \binom{an+bn}{an} \bmod \mathcal{P} \tag{11.12}$$

whenever $0 < a, b, a+b < m$. Since the left hand side is an element in $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, the congruence is even valid modulo $\mathfrak{P} = \mathcal{P} \cap \mathcal{O}_K$. Observe that this contains the results of Corollaries 6.6, 7.6 and Exercise 9.1 as special cases. Also observe that this congruence is compatible with Proposition 4.28 since the binomial coefficient on the right hand side of (11.12) is divisible by p if and only if $a + b = m - 1$ (under the restrictions $0 < a, b, a+b < m$).

11.4 Class Groups of Abelian Number Fields

Our first application will exploit the fact that the Stickelberger relation can be regarded as a statement about the class group: for every prime ideal $\mathfrak{p}$ in $\mathcal{O} = \mathbb{Z}[\zeta_m]$ prime to m, the ideal $\mathfrak{p}^{m\theta}$ is principal, because it is generated by $G(\chi)^m$, where χ is a character of order m on $(\mathcal{O}/\mathfrak{p})^\times$.

Stickelberger's Theorem

Let $K/\mathbb{Q}$ be a finite abelian extension with Galois group G and conductor m. Let σ_a denote the restriction of the automorphism $\zeta_p \longmapsto \zeta_p^a$ of $M = \mathbb{Q}(\zeta_m)$ to K. Then

$$\theta = \theta(K) = \frac{1}{m} \sum_{\substack{0<a<m \\ (a,m)=1}} a\sigma_a^{-1} \in \mathbb{Q}[G]$$

is called the *Stickelberger element* corresponding to K. Clearly $\theta(K)$ is the restriction of $\theta(M)$ to K.

Now we claim that $(b - \sigma_b)\theta \in \mathbb{Z}[G]$ for integers $b \in \mathbb{Z}$ such that $(b, m) = 1$: in fact, from $\sigma_b \sigma_{ab}^{-1} = \sigma_a^{-1}$ we deduce that

$$(b - \sigma_b)\theta = \sum_{(a,m)=1} \Big(b\Big\langle \frac{a}{m} \Big\rangle - \Big\langle \frac{ba}{m} \Big\rangle \Big) \sigma_a^{-1},$$

and this element of $\mathbb{Q}[G]$ has integral coefficients. This allows us to define the *Stickelberger ideal* $I_0(K)$ as the ideal in $\mathbb{Z}[G]$ generated by elements of the form $(b - \sigma_b)\theta$. We also use the name Stickelberger ideal for $I(K) = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$. We have already seen that $I_0(K) \subseteq I(K)$; unfortunately, these ideals are different in general (see Exercise 11.22). Nevertheless we have

Lemma 11.13. *If $K = \mathbb{Q}(\zeta_m)$ is a full cyclotomic field, then $I(K) = I_0(K)$.*

Proof. We already know that $I_0(K) \subseteq I(K)$ for any abelian field K, so it is sufficient to prove the converse. To this end, take any $\beta = \sum_t b_t \sigma_t \in \mathbb{Z}[G]$ with the property $\beta\theta \in \mathbb{Z}[G]$; we have to show that $\beta\theta \in I_0(K)$. The familiar trick of substituting $a = ct$ gives

$$\beta\theta \;=\; \Big(\sum_t b_t \sigma_t \Big) \Big(\sum_a a \sigma_a^{-1} \Big) \;=\; \sum_c \Big(\sum_t \Big\langle \frac{ct}{m} \Big\rangle b_t \Big) \sigma_c^{-1}.$$

Since K is the full cyclotomic field, the automorphisms σ_c are all different, and we can deduce that the coefficient of σ_1 must be an integer, i.e. that $\sum_t tb_t \equiv 0 \bmod m$. But now $\beta\theta = \Big(\sum_t b_t\sigma_t\Big)\theta = \sum_t b_t(t - \sigma_t)\theta + \sum_t tb_t\theta$; the first sum is clearly in $I_0(K)$, the second is an integral multiple of $m\theta = (m + 1 - \sigma_{m+1})\theta$ and therefore also lies in $I_0(K)$. □

Stickelberger used Gauss sums to construct annihilators of the ideal class groups of cyclotomic fields; his result looks quite innocent:

Theorem 11.14. *(Stickelberger's Theorem) Let $K/\mathbb{Q}$ be an abelian extension. Then the Stickelberger ideal $I(K)$ annihilates* $\mathrm{Cl}\,(K)$.

Thus if $\alpha \in \mathbb{Z}[G]$, where $G = \mathrm{Gal}\,(K/\mathbb{Q})$, is such that $\alpha\theta \in \mathbb{Z}[G]$, then $c^\alpha = 1$ for any ideal class $c \in \mathrm{Cl}\,(K)$. In other words: any element of $\mathbb{Z}[G]$ that kills the denominator of the Stickelberger elementattached to $K/\mathbb{Q}$ also kills the class group of K. Let us admit right away that Theorem 11.14 is useless for real abelian fields, because then $\sigma_a = \sigma_{-a}$, thus $\theta = \frac{1}{m}\sum a\sigma_a^{-1} = \frac{1}{m}\sum_{a<m/2}[a + (m-a)]\sigma_a^{-1} = \sum a < m/2\sigma_a^{-1}$, and this last expression is the relative norm from $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$: this clearly kills the ideal class of any intermediate field since $\mathbb{Q}$ has class number 1.

Proof of Theorem 11.14. Let m be the conductor of K; then we have $K \subseteq M = \mathbb{Q}(\zeta_m)$. For a prime ideal $\mathfrak{p} \nmid m$ in M, let $\chi = \chi_\mathfrak{p} = (\frac{\cdot}{\mathfrak{p}})_m^{-1}$ be the corresponding m-th power character. Then we know that $G(\chi)^m = \mathfrak{p}^{m\theta}$ is principal in M, and since the class group is generated by classes of prime ideals coprime to m (any ideal class contains an ideal coprime to any given ideal), we conclude that $m\theta$ annihilates $\mathrm{Cl}\,(M)$. Our first aim is to show that this holds for any $\beta\theta \in I(M)$ (not just for $\beta = m$), and then we will have to pull everything back to $K \subseteq M$.

So assume that we are given a $\beta \in \mathbb{Z}[\Gamma]$ such that $\beta\theta \in \mathbb{Z}[\Gamma]$, where $\Gamma = \mathrm{Gal}\,(M/\mathbb{Q})$. We want to show that $\mathfrak{a}^{\beta\theta}$ is principal for any integral ideal $\mathfrak{a}$ in M; clearly it is sufficient to prove this for ideals coprime to m. To this end, write $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}$ and put $\gamma = \prod_\mathfrak{p} G(\chi_\mathfrak{p})$. Then $\mathfrak{a}^{m\beta\theta} = (\gamma^{m\beta})$ is a principal ideal in M. Put $\alpha = \gamma^{m\beta}$ and $L = M(\sqrt[m]{\alpha})$. Then L/M is a Kummer extension; moreover, $(\gamma^\beta) = \mathfrak{a}^{\beta\theta}$ is an integral ideal in M since $\beta\theta \in \mathbb{Z}[\Gamma]$, hence (α) is an m-th ideal power and therefore L/M is unramified outside m. On the other hand, $L \subseteq M(\zeta_P)$, where P is the product of primes below the prime ideals $\mathfrak{p}$ dividing $\mathfrak{a}$, and every subextension Λ/M of $M(\zeta_P)/M$ ramifies at some p. Since $p \nmid m$, this implies that $L = M$, hence $\gamma^\beta \in M$, and we have shown that $\beta\theta$ annihilates $\mathrm{Cl}\,(M)$.

Now assume that $\mathfrak{a}$ is an integral ideal in K; then $\mathfrak{a}^\sigma = \mathfrak{a}$ for any $\sigma \in \mathrm{Gal}\,(M/K)$. In particular, σ permutes the prime ideals $\mathfrak{p}$ that divide $\mathfrak{a}$. Let s be an automorphism of $M(\zeta_p)/\mathbb{Q}(\zeta_p)$ whose restriction to M is σ (note that, in particular, $\zeta_p^s = \zeta_p$); this is possible since $p \nmid m$. Then right from the definition of a Gauss sum we deduce that $G(\chi_\mathfrak{p})^s = G(\chi_{\mathfrak{p}^\sigma})$. But this implies that γ^β is fixed by σ, hence $\gamma^\beta \in K$ and $\beta\theta(K)$ kills $\mathrm{Cl}\,(K)$. □

A) Quadratic Fields It might seem that this result is not what we wanted, because we were looking for an *integer* annihilating $\mathrm{Cl}\,(K)$, not some element $\beta\theta$ in the group ring $\mathbb{Z}[G]$. But consider an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d}\,)$ with discriminant $d \neq -3, -4, -8$. If we put

$$R = \sum_{\substack{(d/r)=+1 \\ 1 \leq r < d}} r, \quad N = \sum_{\substack{(d/n)=-1 \\ 1 \leq n < d}} n,$$

then $\theta(K) = \frac{1}{|d|}(R + \sigma N)$, where σ is the nontrivial automorphism of $K/\mathbb{Q}$. The definition of θ implies that $|d|\theta \in \mathbb{Z}[G]$; actually, much more is true:

Lemma 11.15. *For any discriminant d of a complex quadratic number field, R and N are divisible by d unless $d \in \{-3, -4, -8\}$.*

Proof. If $d = -\ell$ with $\ell > 3$ prime, this is trivial: choose $a \not\equiv 1 \bmod \ell$ such that $(d/a) = +1$ and observe that $aR \equiv R \bmod \ell$.

Now assume that $d = d'm$ for a prime discriminant d' and some $m \neq \pm 1$. Let $C = \{a + d\mathbb{Z} : (d/a) = +1\}$ be the group of quadratic residues modulo d and consider the homomorphism $\pi : C \longrightarrow (\mathbb{Z}/d'\mathbb{Z})^\times$. Since π is onto, $\#\ker\pi = \frac{1}{2}\phi(m')$, so among the $\frac{1}{2}\phi(d)$ summands in R, exactly $\frac{1}{2}\phi(m')$ reduce modulo d' to a given element in $(\mathbb{Z}/d'\mathbb{Z})^\times$. Thus we see $R \equiv \frac{1}{2}\phi(m')\big(\sum_{(a,d')=1} a\big) \bmod d'$. But if $d' = \pm\ell$ is an odd prime, the last sum is $1 + 2 + \ldots + \ell - 1 = \frac{1}{2}\ell(\ell - 1) \equiv 0 \bmod \ell$, if $d' = -4$, it is $1 + 3 \equiv 0 \bmod 4$, and if $d' = \pm 8$, it is $1 + 3 + 5 + 7 \equiv 0 \bmod 8$. This proves our claims. □

Thus $\theta(K) \in \mathbb{Z}[G]$ for these d, hence Stickelberger's theorem says that $\theta(K) = (R + \sigma N)/d$ annihilates $\mathrm{Cl}\,(K)$. But so does $1 + \sigma$, hence $\mathrm{Cl}\,(K)$ is also killed by $h = \frac{1}{|d|}|R - N|$:

Proposition 11.16. *Let $d < -4$ be a discriminant of an imaginary quadratic number field. Then $h = \frac{N-R}{d}$ annihilates the ideal class group of $k = \mathbb{Q}(\sqrt{d}\,)$, i.e., the h-th power of any ideal in $\mathcal{O}_k$ is principal.*

Note that we have proved that the imaginary quadratic number fields with discriminant $d = -3$ or $d = -4$ have class number 1 in Chapters 6 and 7 by using Jacobi sums, and that the corresponding result for $d = -8$ was shown to hold in Chapter 9 using Eisenstein sums.

B) Quartic Fields Proposition 11.16 is just the tip of an iceberg; in order to show what can be done and to get a feeling for the problems yet to solve, let us look at the complex cyclic quartic fields K of conductor f. Recall that K is a CM-field, that is a totally complex quadratic extension of a totally real number field K^+. For CM-fields K, the *minus* or *relative class group* $\mathrm{Cl}^-(K)$ is defined as the kernel of the norm map $N_{K/K^+} : \mathrm{Cl}\,(K) \longrightarrow \mathrm{Cl}\,(K^+)$. If we let σ denote a generator of $\mathrm{Gal}\,(K/\mathbb{Q})$, then $1 + \sigma^2 = j_{K^+\hookrightarrow K} \circ N_{K/K^+}$, where $j_{K^+\hookrightarrow K} : \mathrm{Cl}\,(K^+) \longrightarrow \mathrm{Cl}\,(K)$ is the canonical transfer of ideal classes. In particular, $1 + \sigma^2$ kills $\mathrm{Cl}^-(K)$ since N_{K/K^+} does.

Instead of just two sums N and R as in the quadratic case, here we have four of them: let ψ be an odd character (that is, $\psi(-1) = -1$; recall that K is complex) of order 4 on $(\mathbb{Z}/f\mathbb{Z})^\times$; then $C_j = \sum_{\psi(a)=i^j} a$. We claim that $C_j \equiv 0 \bmod f$ unless $f \in \{5, 16\}$. This is easily checked for prime power conductors, and if f is not a prime power, we use the same argument as in the quadratic case. Thus we can write $C_j = fD_j$ for integers D_j. Then Stickelberger's theorem says that $\theta = D_0 + D_1\sigma + D_2\sigma^2 + D_3\sigma^3$ kills $\mathrm{Cl}\,(K)$ since $\theta \in \mathbb{Z}[G]$. On the other hand, $1+\sigma^2$ kills $\mathrm{Cl}^{\,-}(K)$, hence so does $(D_0-D_2)+(D_1-D_3)\sigma$ (this follows from $\theta \equiv (D_0 - D_2) + (D_1 - D_3)\sigma \bmod (1 + \sigma^2)$). Now we use the following lemma:

Lemma 11.17. *Let $G = \langle\sigma\rangle$ be a cyclic group of order 4 and assume that the G-module R is annihilated by $1+\sigma^2$ and $a+b\sigma \in \mathbb{Z}[G]$. Then R is annihilated by $a^2 + b^2$.*

Proof. Applying σ to the relation $c^a c^{b\sigma} = 1$ and using the fact that $c^{\sigma^2} = c^{-1}$ we get $1 = c^{a\sigma}c^{b\sigma^2} = c^{a\sigma}c^{-b}$. Raising this to the b-th power we find $1 = c^{-b^2}c^{ab\sigma} = c^{-b^2}c^{-a^2}$, and this proves our claim that $a^2 + b^2$ kills G. □

Using this lemma in the case at hand we find that $(D_0-D_2)^2+(D_1-D_3)^2$ kills $\mathrm{Cl}^{\,-}(K)$. Finally we claim that $h^- = \frac{1}{2}[(D_0 - D_2)^2 + (D_1 - D_3)^2]$ is an integer. But $C_0+C_1+C_2+C_3 = \sum a+\sum(f-a)$, where the sums are over all $1 \le a < f/2$ with $(a, f) = 1$ (the summand $a = f/2$ does never occur: either f is odd, or f is even and $f/2 \notin (\mathbb{Z}/f\mathbb{Z})^\times$). Since there are $\phi(f)/2$ summands, we find $C_0+C_1+C_2+C_3 = f\phi(f)/2$, hence $D_0+D_1+D_2+D_3 = \phi(f)/2$. But $\phi(f)/2$ is even, since f is either divisible by a prime $\equiv 1 \bmod 4$ or divisible by 16. This implies that $D_0 - D_2$ and $D_1 - D_3$ have the same cardinality, and therefore h^- is an integer. We have proved:

Proposition 11.18. *Let $K/\mathbb{Q}$ be a cyclic quartic field with conductor $f \ne 5, 16$ and Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$; let $\psi \in G^\wedge$ be an odd character of order 4 on $(\mathbb{Z}/f\mathbb{Z})^\times$, define C_j as the sum of all $t \in (\mathbb{Z}/f\mathbb{Z})^\times$ with $\psi(t) = i^j$ and put $C_j = fD_j$. Then $2h^-$ annihilates the minus class group of K, where*

$$h^- = \frac{1}{2}\left((D_0 - D_2)^2 + (D_1 - D_3)^2\right).$$

It is not too hard to prove more general versions; unfortunately, it seems, the method we have presented only shows that some power of 2 times h^- kills $\mathrm{Cl}^{\,-}(K)$ for general abelian extensions $K/\mathbb{Q}$. It seems that even in the case of full cyclotomic fields of prime power conductor, the best result that can be achieved with algebraic methods is that $2h^-$ kills the minus class group. For prime power conductors, one can use genus theory to show that, in Proposition 11.18, the class number $h(K)$ is odd, hence that h^- annihilates the minus class group of K.

Herbrand's Theorem

Herbrand's Theorem is a result on the fine structure of the p-class group of $\mathbb{Q}(\zeta_p)$, strengthening previous classical results in a very beautiful way. The story starts, predictably, with Kummer.

A) Kummer and Hecke In his letter to Kronecker (May 17, 1847), Kummer conjectured that the class number h of $K = \mathbb{Q}(\zeta_p)$ is divisible by p (such primes he called *irregular*; primes not dividing h were called *regular*) if p divides the numerator of one of the Bernoulli numbers B_2, B_4, ... , B_{p-3}. He also conjectured that units congruent to a rational integer modulo p must be p-th powers if $p \nmid h$ (this would later become known as *Kummer's Lemma*) and expressed his hope that the first conjecture would imply the second. In a letter to Dirichlet (Sept. 16, 1847) he not only sketched a proof of these conjectures but also introduced the class number h^+ of the maximal real subfield $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of K and showed that $h^+ \mid h$:

Theorem 11.19. *A prime p is irregular if and only if p divides the numerator of one of the Bernoulli numbers B_2, B_4, ... , B_{p-3}. Moreover, the quotient $h^- = h/h^+$ is integral, and $p \mid h^+$ only if $p \mid h^-$.* □

In another letter to Kronecker (Dec. 28, 1849), Kummer announced that he had found a unit $\varepsilon \in \mathbb{Z}[\zeta_{37}]$ that is congruent to a rational integer modulo p but not an p-th power (in modern terminology: $K(\sqrt[37]{\varepsilon}\,)/K$ is an unramified cyclic extension of $K = \mathbb{Q}(\zeta_{37})$, or, since $h_{37} = 37$: the Kummer extension $K(\sqrt[37]{\varepsilon}\,)$ is the Hilbert class field of K).

The number $i(p)$ of indices $i \le \frac{p-3}{2}$ such that $p \mid B_{2i}$ is called the *index of irregularity*. It is very hard to find good bounds on $i(p)$; see Metsänkylä [Met] for more.

Kummer also introduced the relative class number h_p^- of $K = \mathbb{Q}(\zeta_p)$: let h_p and h_p^+ denote the class numbers of K and its maximal real subfield $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, respectively. Then $h_p = h_p^+ h_p^-$, and both factors are integers. Kummer's observation that $p \mid h_p^+$ implies $p \mid h_p^-$ was later refined by Hecke [Hec], who used the class field theory of Furtwängler to show

Proposition 11.20. *We have* $\operatorname{rank} \operatorname{Cl}_p(K^+) \le \operatorname{rank} \operatorname{Cl}_p^-(K)$. □

As a corollary of the two preceding theorems we note that $p \mid h_p$ if and only if $p \mid B_2 B_4 \cdots B_{p-3}$. This prompts the question whether the p-part of the minus class group of $\mathbb{Q}(\zeta_p)$ can be broken into smaller pieces such that the nontriviality of such a piece is controlled by the p-divisibility of a corresponding Bernoulli number.

B) Idempotents Let K be a totally complex abelian number field with maximal real subfield K^+; then the restriction J of complex conjugation to K generates $H = \operatorname{Gal}(K/K^+)$. Moreover, J acts on the class group, and for each odd prime p there is a decomposition of $\operatorname{Cl}_p(K)$ into a plus and a minus part.

This decomposition can be put into a quite general framework: let R be a commutative ring with 1, and M an R-module. An element $e \in R$ is called an *idempotent* if $e^2 = e$. If e is an idempotent, then so is $1-e$: in fact, $(1-e)^2 = 1 - 2e + e^2 = 1 - e$ as desired. The existence of idempotents allows us to decompose R-modules M into smaller pieces: for $m \in M$, we get $m = 1m = (e + 1 - e)m = em + (1-e)m$, so M is the sum of the submodules (!) eM and $(1-e)M$. Moreover, this sum is direct: this is due to the fact that e and $1-e$ are orthogonal idempotents, that is, we have $e(1-e) = 0$. Thus if $m \in eM \cap (1-e)M$, then $m = em_1 = (1-e)m_2$, hence $m = em_1 = e^2m_1 = e(1-e)m_2 = 0m_2 = 0$.

As a simple example, assume that a group $H = \{1, J\}$ acts on M; define $M^+ = \{m \in M : Jm = m\}$ and $M^- = \{m \in M : Jm = -m\}$. If M has odd order n, then M is a $\mathbb{Z}/n\mathbb{Z}$-module, and since 2 has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, the element $e = \frac{1+J}{2}$ is in $R = (\mathbb{Z}/p^n\mathbb{Z})[H]$. Next $J^2 = 1$ implies that $e^2 = e$, that is, e is an idempotent in R. As we have seen, this implies $M = eM \oplus (1-e)M$; moreover, $eM \subseteq M^+$ since $Je = e$, and $(1-e)M \subseteq M^-$ since $J(1-e) = -(1-e)$, and this implies that we actually have $M^+ = eM$ and $M^- = (1-e)M$. In the case $p = 2$, there is a weak substitute in form of Exercise 11.11.

The prototype for such considerations is the decomposition of the class group $\mathrm{Cl}_p(K)$, p an odd prime, into plus and minus parts. Now $\mathrm{Cl}_p(K)$ is not only acted upon by H but by the whole Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Since this is an abelian group, it contains many idempotents:

Proposition 11.21. *Let G be a finite abelian group with character group $G^\wedge = \mathrm{Hom}(G, \mathbb{C}^\times)$. Let R be an integral domain containing $\chi(\sigma)$ for all $\sigma \in G$, and suppose that $\#G$ is a unit in R. Then the elements*

$$\varepsilon_\chi = \frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in R[G]$$

form a complete set of orthogonal idempotents of $R[G]$, that is we have $\varepsilon_\chi^2 = \varepsilon_\chi$ (idempotent), $\varepsilon_\chi\varepsilon_\psi = 0$ for $\chi \neq \psi$ (orthogonal), and $\sum_{\chi \in \widehat{G}} \varepsilon_\chi = 1$ (complete). Moreover, $\tau\varepsilon_\chi = \chi(\tau)\varepsilon_\chi$ for every $\tau \in G$.

Proof. This is a straightforward verification. □

For understanding Herbrand's Theorem, it is sufficient to look at the quotient group $\mathcal{C} = \mathrm{Cl}(K)/\mathrm{Cl}(K)^p$ of the class group. This is clearly an $\mathbb{F}_p[G]$-module, and the character group $G^\wedge$ is generated by the character ω that maps $\sigma_a \in G$ to $a \bmod p$ (this becomes a character in the above sense upon identifying $\mathbb{F}_p^\times$ with μ_{p-1}). Writing $e_i := \varepsilon_{\omega^i}$ for $1 \leq i \leq p-1$, we find that

$$e_i = \frac{1}{p-1} \sum_{t=1}^{p-1} t^i \sigma_t^{-1}$$

are the idempotents constructed above. For any $\mathbb{F}_p[G]$-module M we can therefore define $M_i = e_i M$. It is a formal consequence of the properties of complete sets of orthogonal idempotents that we have $M = M_1 \oplus \ldots \oplus M_{p-1}$: the existence of the sum is deduced from $1 = \sum e_i$, the fact that the sum is direct follows from the orthogonality relations in the same way as in the special case of the idempotents e and $1 - e$ above.

It is an easy exercise to show that $M^- = M_1 \oplus \ldots \oplus M_{p-2}$ and $M^+ = M_2 \oplus \ldots \oplus M_{p-1}$, or, equivalently, that $\frac{1-J}{2} = \sum_{\chi \text{ odd}} e_\chi$ and $\frac{1+J}{2} = \sum_{\chi \text{ even}} e_\chi$ (recall that $J = \sigma_{-1}$). In particular, the decomposition of M into eigenspaces is finer than the one into a plus and minus part, at least for $p > 3$.

C) Pollaczek, Takagi, Herbrand and Ribet Let us recall the situation: We have an odd prime p, the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, and its Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$; we want to study the action of G on the p-class group $\mathrm{Cl}_p(K)$. Using the idempotents of $\mathbb{F}_p[G]$ introduced above we get the decomposition

$$\mathcal{C} = \mathrm{Cl}\,(K)/\mathrm{Cl}\,(K)^p = \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_{p-1},$$

where the submodules $\mathcal{C}_i = \varepsilon_i \mathcal{C}$ can be described more concretely by

$$\mathcal{C}_i = \{c \in \mathcal{C} : \sigma_t(c) = c^{t^i} \text{ for } 1 \le t \le p-1\}.$$

Thus Hecke's result (Proposition 11.20) can be expressed by saying that $\mathrm{rank}\,\mathcal{C}^+ \le \mathrm{rank}\,\mathcal{C}^-$. By studying the interplay between Kummer theory and class field theory, Leopoldt [Leo] was able to refine this inequality considerably:

Theorem 11.22. *We have* $\mathrm{rank}\,\mathcal{C}_{2n} \le \mathrm{rank}\,\mathcal{C}_{p-2n} \le 1 + \mathrm{rank}\,\mathcal{C}_{2n}$ *for all* $1 \le n \le \frac{p-3}{2}$. □

Actually this is only a special case of Leopoldt's famous 'Spiegelungssatz' (reflection theorem).

In general it is hard to tell which of the subspaces $\mathcal{C}_i$ are trivial and which are not; the following theorem due to Pollaczek [Pol], Takagi [Tak] and Herbrand [Her] refines Kummer's Theorem 11.19:

Theorem 11.23. *We have* $\mathcal{C}_1 = 1$, *and for odd integers* $3 \le i \le p-2$, $p \nmid B_{p-i}$ *implies* $\mathcal{C}_i = 1$.

This shows that the p-divisibility of certain Bernoulli numbers controls the minus class group $\mathrm{Cl}_p^-(K)$ in a very precise way. The proof that $\mathcal{C}_1 = 1$ is actually quite easy: if $c \in \mathcal{C}_1$, then $c^{\sigma_t} = c^t$, hence, by Stickelberger's theorem, $1 = c^{\sum t\sigma_t^{-1}} = c^{\sum tt^{-1}} = c^{p-1} = c^{-1}$, and the claim follows.

The general case is more difficult: in order to make the proof work, we have to use the Stickelberger element θ: its denominator p does not allow us to continue using $\mathbb{F}_p G$.

We therefore have to replace the $\mathbb{F}_p G$-module $\mathcal{C}$ by the $\mathbb{Z}_p G$-module $\mathrm{Cl}_p(K)$; this is'nt really more than a switch of language: let M be any finite abelian p-group of order p^{m+1} on which a group G acts; then we can make M into a $\mathbb{Z}_pG$-module by letting $\alpha = a_0 + a_1p + \ldots + a_mp^m + \ldots \in \mathbb{Z}_p$ (with $0 \le a_j \le p-1$) act on M via $m^\alpha = m^{a_0+a_1p+\cdots+a_mp^m}$ for any $m \in M$.

Both interpretations are compatible: the action of a group ring RG on an abelian p-group M gives rise to a homomorphism $RG \longrightarrow \mathrm{Aut}\,(M)$, and we have a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}_pG \arrow[r] \arrow[d, "\pi"] & \mathrm{Aut}\,(M) \arrow[d] \\
\mathbb{F}_pG \arrow[r] & \mathrm{Aut}\,(M/M^p)
\end{tikzcd}$$

with $\pi : \mathbb{Z}_pG \longrightarrow \mathbb{F}_pG$ being induced by reduction modulo p.

In order to lift the idempotents from $\mathbb{F}_pG$ to $\mathbb{Z}_pG$ we have to replace the cyclotomic character ω by the Teichmüller character (that we continue to denote by ω) defined as follows: for any $1 \le a \le p-1$, the sequence a, a^p, a^{p^2}, $\ldots$ converges in $\mathbb{Z}_p$; its limit $\omega(a)$ satifies $\omega(a) \equiv a \bmod p$ and $\omega(a)^{p-1} = 1$, that is: it is contained in the subgroup $\mu_{p-1} \subset \mathbb{Z}_p^\times$. Using the isomorphism $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ we can view ω as a character $\mathrm{Gal}\,(K/\mathbb{Q}) \longrightarrow \mu_{p-1}$, and then the idempotents $e_i = \varepsilon_{\omega^i}$ are elements of $\mathbb{Z}_pG$, as are the generalized Bernoulli numbers that will occur in a moment.

Back to the proof of Herbrand's theorem: we know from Stickelberger's Theorem that $(b - \sigma_b)\theta$ kills the class group $\mathrm{Cl}\,(K)$; in particular it kills $\mathcal{C}$. Thus $\mathcal{C}_i$ is annihilated by $(b - \sigma_b)\theta e_i$. Now $\sigma_a e_i = \omega^i(a)e_i$ implies that

$$\theta e_i = \Big(\frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-i}(a)\Big)e_i = B_{1,\omega^{-i}}e_i, \tag{11.13}$$

hence $\mathcal{C}_i$ is killed by $(b-\omega^i(b))B_{1,\omega^{-i}}e_i$. Choose b in such a way that $b-\omega^i(b)$ is not divisible by p (for example, take b to be a primitive root modulo p; then $\omega^i(b) \equiv g^i \bmod p$, and $p \mid (g - g^i)$ if and only if $i \equiv 1 \pmod{p-1}$, which is not the case here); since e_i is an automorphism on $\mathcal{C}_i$ we see that $\mathcal{C}_i$ is killed by $B_{1,\omega^{-i}}$. Finally, putting $n = p - i - 1$ in the congruence

$$\frac{1}{n+1}B_{n+1} \equiv B_{1,\omega^n} \bmod p. \tag{11.14}$$

(see Washington [Was1, Corollary 5.13]) and observing that $\omega^{p-1} = 1\!\!1$ gives $B_{1,\omega^{-i}} \equiv \frac{1}{p-i}B_{p-i} \bmod p$. This shows that $\mathcal{C}_i$ is killed by B_{p-i}, and Herbrand's theorem follows.

Takagi [Tak] and Herbrand [Her] showed moreover that if one assumes the truth of Vandiver's conjecture that p does not divide the class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then the converse also holds: this is done by writing down the corresponding p-class fields explicitly as Kummer extensions generated by p-th roots of certain cyclotomic units; Vandiver's conjecture is needed for securing that these units aren't p-th powers.

Example. For $p = 37$ we find that B_{32} is the only Bernoulli number with index ≤ 34 divisible by 37. Since $h_{37}^- = 37$, we conclude that the minus class group of $K = \mathbb{Q}(\zeta_{37})$ consists only of $\mathcal{C}_5$. In particular, we see that $\sigma_2(c) = c^{32}$ for each ideal class $c \in \mathrm{Cl}^-(K)$.

Using deep properties of modular curves, Ribet [Rb1] succeeded in removing Vandiver's conjecture from the converse of Herbrand's theorem:

Theorem 11.24. *For odd integers $3 \le i \le p-2$, the relation $p \mid B_{p-i}$ implies $\mathcal{C}_i \ne 1$.* □

For an exposition of Ribet's proof without the technical details, see Tamme [Ta]. The explicit construction of the class fields corresponding to nontrivial $\mathcal{C}_i$ was studied by Harder & Pink [HP] as well as by Harder's students Lippert [Lip] and Kleinjung [Klj]. Generalizations to cyclotomic fields of conductor pq were given by Kamienny [Ka].

Gut [Gut] studied a similar situation in 1951: consider the fields $L = \mathbb{Q}(\zeta_{4n})$ and $K = \mathbb{Q}(\zeta_n)$; the relative class group $\mathrm{Cl}\,(L/K)$ is defined to be the kernel of the norm map $N_{L/K} : \mathrm{Cl}\,(L) \longrightarrow \mathrm{Cl}\,(K)$; let $C = \mathrm{Cl}_p(L/K)$ be its p-Sylow subgroup. Next define the *Euler numbers* E_n by

$$\sum_{n=0}^{\infty} E_n \frac{x^n}{n!} = \frac{2}{e^x + e^{-x}};$$

actually Euler numbers are essentially generalized Bernoulli numbers since $E_n = \frac{2}{n+1} B_{n+1,\chi}$, where χ is the nontrivial Dirichlet character modulo 4. Then Gut showed that $\#C$ is divisible by p if and only if one of the Euler numbers $E_2, \ldots, E_{p-3}$ is divisible by p. Kleboth [Kle] proved the analogous result over $\mathbb{Q}(\zeta_3)$. The natural question whether this result can be improved in the direction of Herbrand's theorem was only studied after Mazur and Wiles had proved the main conjecture of Iwasawa theory which contained such an extension of Gut's result as a very special case.[1] Recently, Ernvall [Er2] has proved such a generalization of Herbrand's theorem using the elementary techniques of Herbrand.

The Stickelberger Ideal

The most attractive results about the structure of class groups of abelian fields are known only for cyclotomic fields of prime power conductor, and in this case the desired result follows from the computation of the index of the Stickelberger ideal:

Theorem 11.25. *(The Index of the Stickelberger Ideal) Let $m = p^n$ be a prime power, $K = \mathbb{Q}(\zeta_m)$, $G = \mathrm{Gal}(K/\mathbb{Q})$, $R = \mathbb{Z}[G]$, $\theta = \theta(K)$ the corresponding Stickelberger element, and $I = R \cap R\theta$ the Stickelberger ideal. Moreover, let $J = \sigma_{-1}$ denote complex conjugation, and define*

[1] Karl Rubin kindly explained that to me in an email from July 29, 1998.

$$R^- = \{x \in R \mid Jx = -x\}, \quad I^- = I \cap R^-.$$

Then

$$(R^- : I^-) = h^-(K) \ := \ Qw \prod_{\chi \ odd} \left\{ -\frac{1}{2f_\chi} \sum_{t=1}^{f_\chi - 1} \chi(t)t \right\}. \tag{11.15}$$

The analytic class number formula says that the number $h^-(K)$ defined above coincides with the minus class number $h^-(K) = \#\mathrm{Cl}^-(K)$ for any abelian extension of $\mathbb{Q}$. Here $Q = (E_K : W_K E_{K^+})$ denotes Hasse's unit index, which is known to be trivial for cyclotomic fields of prime power conductor, and in general takes only the values 1 or 2 (see Exercise 11.10). The product is over all odd characters of the character group $X(K/\mathbb{Q})$ associated to abelian extensions of $\mathbb{Q}$ in Section 4.5. Using the generalized Bernoulli numbers defined in Equation (10.16) we can also express h^- in the form

$$h^- = Qw \prod_{\chi \ odd} \Big(-\frac{1}{2} B_{1,\chi} \Big).$$

Note that these h^- coincide with the integers defined in Propositions 11.16 and 11.18 above (see Exercise 11.23).

Let us give a few examples. Assume that p is an odd prime and let $K = \mathbb{Q}(\zeta_{p^n})$. We claim that Theorem 11.25 provides us with an algebraic proof that $h^-(K)$ annihilates the odd part of $\mathrm{Cl}^-(K)$. In fact, we know $\mathrm{Cl}_p^-(K) = \mathrm{Cl}_p(K)^{1-J} = \mathrm{Cl}_p(K)^{R^-}$, so for any $c \in \mathrm{Cl}_p^-(K)$, we find $c^{h^-} \in \mathrm{Cl}(K)^{I^-}$, because $h^- = (R^- : I^-)$; but I^- annihilates the ideal class group of K, hence h^- annihilates $\mathrm{Cl}_p^-(K)$ for every odd prime p. For $p = 2$ the result is not as strong: from Exercise 11.11 we know that $\mathrm{Cl}_2^-(K)^2 \subseteq \mathrm{Cl}_2(K)^{(1-J)}$, so the above reasoning only shows that $2h^-$ annihilates $\mathrm{Cl}_2^-(K)$.

The proof that $h^-(K) = (R^- : I^-)$ also shows that $h^-(K)$ is an integer: a direct integrality proof for general abelian extensions was given by Hasse [Has1].

For the proof of Theorem 11.25 we need a few concepts. Exercise 11.13 generalizes the notion of an index of free abelian groups (lattices, to be exact). From Exercise 11.14 we will also borrow the fact that if V is a $\mathbb{Q}$-vector space and $T : V \longrightarrow V$ an invertible endomorphism, then $(A : TA) = |\det T|$ for any lattice A in V.

Proof of Theorem 11.25. We will split up the index $(R^- : I^-)$ into more manageable parts. To this end, we put $\mathcal{S} = \{\alpha \in R : \alpha\theta \in R\}$, so $I = R \cap R\theta = \theta\mathcal{S}$. We also introduce the $\mathbb{Q}$-vector space $V = \mathbb{Q}[G]^- = 2e^-\mathbb{Q}[G] = \{\alpha \in \mathbb{Q}[G] : (1 + J)\alpha = 0\}$, where $2e^- = 1 - J \in \mathbb{Z}[G]$, and the linear map $T : V \longrightarrow V$ defined by $T\alpha = \theta\alpha$. Clearly V is a $\mathbb{Q}$-vector space of dimension $r = \frac{1}{2}\#G$, and R^- is a submodule of V of full rank r. Now

$$(R^- : I^-) \; = \; \frac{(R^- : 2e^-\mathcal{S})(2e^-\mathcal{S} : T(2e^-\mathcal{S}))(T(2e^-\mathcal{S}) : 2I^-)}{(I^- : 2I^-)}.$$

Since I^- has rank r, we see $(I^- : 2I^-) = 2^r$. Moreover, $(2e^-\mathcal{S} : T(2e^-\mathcal{S})) = |\det T|$; in order to compute this determinant, we extend T to a map on $\mathbb{C}[G]^- = \{\alpha \in \mathbb{C}[G] : (1+J)\alpha = 0\}$ and observe that the idempotents e_χ, χ odd, form a basis of $\mathbb{C}[G]^-$ over $\mathbb{C}$. The relation (11.13), when generalized from primes p to prime powers, says that $e_\chi\theta = B_{1,\chi^{-1}}\theta$. Thus the e_χ are eigenvectors of T with eigenvalues $B_{1,\chi^{-1}}$, hence $\det T = \prod_{\chi \text{ odd}} B_{1,\chi^{-1}}$.

All that is left to do now is to compute $(R^- : 2e^-\mathcal{S})$ and $(T(2e^-\mathcal{S}) : 2I^-)$. We define a homomorphism $\phi : R \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ by putting $\phi(\sigma_a) = a + p^n\mathbb{Z}$ and claim that

$$0 \longrightarrow \mathcal{S} \longrightarrow R \xrightarrow{\;\phi\;} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

is an exact sequence. Surjectivity of ϕ being clear, we have to show that $\ker\phi = \mathcal{S}$. Take an $\alpha = \sum x_b\sigma_b \in R$; here and below, the sums are over all $1 \le b < p^n$ with $p \nmid b$. Then

$$p^n\alpha\theta = \sum_a\sum_b a x_b \sigma_a^{-1}\sigma_b \; = \; \sum_c \sigma_c \sum_a a x_{ac}.$$

Now $\alpha \in \mathcal{S}$ means $\alpha\theta \in R$, and this implies that the coefficient of σ_1 in $p^n\alpha\theta$ is divisible by p^n; but then $\sum_a a x_a \equiv 0 \bmod p^n$, hence $\phi(\alpha) = 0$ and $\alpha \in \ker\phi$. Conversely, assume that $\phi(\alpha) = 0$. Since ϕ is a homomorphism, this implies $\phi(\alpha\sigma_c^{-1}) = 0$, hence the coefficient of σ_1 in $\alpha\sigma_c^{-1}\theta$ is an integer; now this coefficient coincides with the coefficient of σ_c in $\alpha\theta$, therefore $\alpha\theta \in R$ and $\alpha \in \mathcal{S}$ as claimed.

Note that $R^- = 2e^-R$, although this is not obvious as 2 is not invertible in $\mathbb{Z}$. In fact it is sufficient to show that $R^- \subseteq 2e^-R$. But $\alpha = \sum x_a\sigma_a \in R^-$, the sum being over all $1 \le a < m$ with $p \nmid a$, implies that $x_a = -x_{m-a}$, hence $\alpha = \sum_a x_a\sigma_a = (1-J)\sum_b x_b\sigma_b$, where b runs over the integers $1 \le b < \frac{m}{2}$ not divisible by p.

Now we use the simple fact that $(A : B) = (A^f : B^f)(A_f + B : B)$, where $f : A \longrightarrow A$ is a group endomorphism and where $B \subseteq A$ is a subgroup of the abelian group A (see Exercise 11.12). Applying this to the situation $A = R$, $B = \mathcal{S}$ and $f = 1 - J$, we find $(R : \mathcal{S}) = (R^- : 2e^-\mathcal{S})$ because the kernel of $1 - J : R \longrightarrow R$ is $(1+J)R \subseteq \mathcal{S}$. Thus $(R^- : 2e^-\mathcal{S}) = p^n$.

Finally we claim that $(T(2e^-\mathcal{S}) : 2I^-) = \delta$ with $\delta = 2$ if p is odd and $\delta = 1$ if $p = 2$; in particular, $\delta \cdot p^n = w$ gives the number of roots of unity in K. Taking this for granted and putting everything together we get

$$\begin{aligned}(R^- : I^-) &= \frac{(R^- : 2e^-\mathcal{S})(2e^-\mathcal{S} : T(2e^-\mathcal{S}))(T(2e^-\mathcal{S}) : 2I^-)}{(I^- : 2I^-)} \\ &= \frac{p^n \cdot |\prod B_{1,\chi^{-1}}| \cdot \delta}{2^r} \; = \; w \prod_{\chi \; odd} \Big(-\frac{1}{2}B_{1,\chi}\Big),\end{aligned}$$

where $w = \# W_K$ denotes the number of roots of unity in K. The fact that the product $\prod_{\chi\ odd}(-\frac{1}{2}B_{1,\chi})$ is positive follows from the analytic class number formula; if you don't want to invoke analytic machinery, take the absolute value on both sides.

In order to study the index $(T(2e^-\mathcal{S}) : 2I^-)$ we introduce a homomorphism $\psi : T(2e^-\mathcal{S}) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by putting $\psi(2e^-\gamma\theta) = \omega(\gamma) + 2\mathbb{Z}$, where $\omega : R \longrightarrow \mathbb{Z}$ induced by mapping σ_a to 1. The identity $2 = 2e^- + 2e^+$ (with $e^+ = 1 + J$) shows that $2e^-\gamma\theta = 2\gamma\theta - 2e^+\gamma\theta$; since $2e^+\theta = N$ is the norm, we have $2e^+ \in \mathcal{S}$, $N \in I$, and $2e^+\gamma\theta = \gamma N = \omega(\gamma)N$. If $\omega(\gamma)$ is even, then this implies that $2e^-\gamma\theta \in 2I \cap R^- = I^-$. Conversely, if $2e^-\gamma\theta \in 2I^-$, then $\omega(\gamma)N \in 2R$, thus $2 \mid \omega(\gamma)$. This proves that $\ker\psi = 2I^-$.

If there is a $\gamma \in \mathcal{S}$ such that $\psi(\gamma)$ is odd, then similarly $2e^-\gamma\theta - N \in 2I$, and then $N \in R \setminus 2R$ implies that $2e^-\gamma\theta \notin 2I^-$, which in turn means that ψ is onto. Now if p is odd, then $p^n \in \mathcal{S}$, so $\gamma = p^n$ does it. If $p = 2$, however, then we claim that ψ is the trivial map. To this end we observe that $(\sum x_b\sigma_b)\theta = (\sum x_b b)\theta$ for $\sum x_b\sigma_b \in R$; since the b's are all odd if $p = 2$, we see that $\sum x_b b \equiv \sum x_b = \omega(\sum x_b\sigma_b) \bmod 2$. In particular, the existence of a $\gamma \in \mathcal{S}$ with odd $\omega(\gamma)$ implies that the odd integer $\omega(\gamma)$ is in $\mathcal{S}$: but $\mathcal{S}$ also contains $m = 2^n$, and since $\mathcal{S}$ is an ideal, it must be equal to R. But this is a contradiction because it would imply $\theta \in R$. This completes our proof. □

Sinnott [Sin] defined a Stickelberger ideal $I(K)$ for general abelian extensions $K/\mathbb{Q}$ in such a way that Theorem 11.25 essentially remains valid; more exactly he showed that $(R^- : S^-) = c^-h^-$ for certain 'dirt factors' c^-. Similar class number formulas hold for the plus part when Stickelberger ideals are replaced by cyclotomic units. Recently, a unified approach combining the plus and minus side was discovered by Anderson [An]. Anderson also inspired a new proof of Sinnott's formulas by Ouyang [Ou] in which Sinnott's quite technical calculations are replaced by arguments using spectral sequences. For computational aspects involving Stickelberger ideals, see Schoof [Sf3].

The fact that the index $(R^- : I^-)$ coincides with the minus class number $h^- = \#\,\mathrm{Cl}^-(K)$ prompts the question whether there is an isomorphism $R^-/I^- \simeq \mathrm{Cl}^-(K)$ as abelian groups (or even as $\mathrm{Gal}\,(K/\mathbb{Q})$-modules). The answer to the second question is no (see Washington [Was1]), and the first question can be answered negatively using the following result due to Jha [Jha, p. 78]:

Proposition 11.26. *Let $p \equiv 3 \bmod 4$ be a prime, $K = \mathbb{Q}(\zeta_p)$, and let R^- and I^- be as above. Moreover, let h be defined as in Proposition 11.16. Then h divides the exponent t of R^-/I^-, and, in particular, $h \mid h^-(K)$.*

Proof. Consider the homomorphism $\lambda : R \longrightarrow \mathbb{Z}$ induced by $\sigma_a \longmapsto (\frac{a}{p})$. Observe that $\lambda(\theta) = h$. Since $1 - J \in R^-$ and t kills R^-/I^-, we have $(1-J)t \in I^- = R^- \cap R\theta$. Thus $(1-J)t = \gamma\theta$ for some $\gamma \in R$, hence $2t = \lambda((1-J)t) = \lambda(\gamma)\lambda(\theta) = \lambda(\gamma) \cdot h$. Now $\lambda(\gamma)$ is an integer, hence h divides $2t$; but h is odd by genus theory, and the claim follows. □

We need another ingredient:

Proposition 11.27. *Let ℓ, q and $p = 2q+1$ be odd primes, and assume that ℓ is a primitive root modulo q. Put $K = \mathbb{Q}(\zeta_p)$ and let h be defined as in Proposition 11.16. Then ℓ does not divide $h^-(K)/h$.*

Proof. We have already seen that $h \mid h^-(K)$, hence $h^-(K)/h$ is an integer. From the definition of $h^-(K)$ and h we find immediately that $h^-(K)/h = 2p\prod_\chi(-\frac{1}{2}B_{1,\chi})$, where the product is over all characters of $\mathbb{F}_p^\times$ with exact order $p-1 = 2q$ (the class number h corresponds to the single odd character of order 2 in the product (11.15)). Now $B_{1,\chi} \in \mathbb{Q}(\zeta_q)$, and the product over all characters of order $2q$ is simply the norm of $B_{1,\psi}$, where ψ is the character defined by $\psi(\ell) = \zeta_{2q}$. But since ℓ is inert in $\mathbb{Q}(\zeta_q)$, the norm of $B_{1,\psi}$ is divisible by ℓ if and only $B_{1,\psi}$ is. But this is easily seen not to be the case: if we write $B_{1,\psi} = \frac{1}{p}\sum_{a=1}^{p-1} a\psi(a)^{-1} = \sum_{j=0}^{q-1} a_j\zeta_q^j$, then $a_0 = \psi(1)+(p-1)\psi(p-1) = 2-p$ and (observe that $\zeta_{2q} = \zeta_q^{(q+1)/2}$) $a_{(q+1)/2} = \ell\psi(\ell)+(p-\ell)\psi(p-\ell) = 2\ell-p$. But a sum $\sum_{j=0}^{q-1} a_j\zeta_q^j$ is divisible by an integer n if and only if n divides all the differences $a_j - a_0$; since $a_{(q+1)/2} - a_0 = 2\ell - p - (2-p) = 2\ell - 2$ and since ℓ is odd, $B_{1,\psi}$ is not divisible by ℓ. □

For a proof that R^-/I^- is not isomorphic to $\mathrm{Cl}^-(K)$ as an abelian group we use the analytic class number formula which says that $h^-(K)$ is the order of $\mathrm{Cl}^-(K)$, and that h is the class number of $k = \mathbb{Q}(\sqrt{-p})$. Now take $\ell = 3$ and let p and q be as above. Then $(K:k) = q$ is not divisible by ℓ, consequently the transfer of ideal classes $j : \mathrm{Cl}(k) = \mathrm{Cl}^-(k) \longrightarrow \mathrm{Cl}^-(K)$ is injective (see Exercise 11.25). If we can find a p such that the 3-class group $\mathrm{Cl}_3(k)$ of k is non-cyclic, then so is $\mathrm{Cl}^-(K)$. If 3 is a primitive root modulo q, then the fact that $3 \nmid h^-/h$ implies that $\mathrm{Cl}_3^-(K) \simeq \mathrm{Cl}_3(k)$. Thus $h/3$ kills $\mathrm{Cl}_3^-(K)$ while the exponent of R^-/I^- is divisible by h: hence R^-/I^- is not isomorphic to $\mathrm{Cl}^-(K)$.

Finding such q is easy: $q = 30689$ (here $\mathbb{Q}(\sqrt{-p})$ has class group $(\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z})$ and $q = 38333$ (here $\mathbb{Q}(\sqrt{-p})$ has class group $(\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z})$ are the two smallest examples.[2]

Brumer and Stark

To some degree, the results of Stickelberger on the annihilation of class groups can be generalized (at least conjecturally) from abelian extensions of $\mathbb{Q}$ to those of arbitrary number fields. So let K/k be an abelian extension of number fields with Galois group $G = \mathrm{Gal}(K/k)$ and conductor $\mathfrak{f} = \mathrm{cond}(K/k)$. Let S denote a finite set of places containing all ramified and all archimedean places, and write $(\mathfrak{a}, S) = 1$ if an integral ideal $\mathfrak{a}$ is not divisible by any finite prime in S. Then define the partial ζ-function

[2] Thanks go to René Schoof and Larry Washington for communicating the ideas that led to these examples (emails from Nov. 13, 1999).

$$\zeta_S(\sigma, s) = \sum_{\substack{(\mathfrak{a},S)=1 \\ (\mathfrak{a},K/k)=\sigma}} N\mathfrak{a}^{-s}. \tag{11.16}$$

Here $(\mathfrak{a}, K/k)$ denotes the Artin symbol. Siegel has shown that the values $\zeta_S(\sigma, 0)$ are rational (this is a deep result!), hence the *Brumer-Stark elements*

$$\theta_{S,K/k} = \theta_{S,G} = \theta_S := \sum_{\sigma \in G} \zeta_S(\sigma, 0)\sigma^{-1} \tag{11.17}$$

are elements of the group ring $\mathbb{Q}[G]$. It follows from work of Deligne & Ribet [DeR] (as well as from Shintani's formulas [Shi]) that the denominator of θ_S is bounded by the number of roots of unity in K; in fact, if we denote the group of roots of unity in K by W_K and put $w = \#W_K$, then

$$w\,\theta_{S,K/k} \in \mathbb{Z}[G]. \tag{11.18}$$

More generally, if some $\xi \in \mathbb{Z}[G]$ kills W_K, then $\xi\theta_{S,K/k} \in \mathbb{Z}[G]$.

Let us see what happens when $k = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_m)$ for some $m \geq 3$. In this case, the Artin symbol $(a, K/\mathbb{Q})$ maps an ideal (a) generated by a positive integer a coprime to m to the element $\sigma_a : \zeta_m \longmapsto \zeta_m^a$ of the Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$. Thus the elements $a \in \mathbb{N}$ whose Artin symbols coincide form a residue class modulo m, and the partial ζ-function defined in (11.16) coincides with the partial ζ-function (10.13) studied in Chapter 10. Here clearly $S = \{\infty\} \cup \{p : p \mid m\}$. Recall that

$$\zeta(\sigma_a, 0) = \frac{1}{2} - \left\langle \frac{a}{m} \right\rangle$$

by Theorem 10.22. This shows that the corresponding Brumer-Stark elements are $\theta_{S,K/k} = \frac{1}{2}\nu - \theta$, where θ is the Stickelberger element defined in (11.11). Note that $\#W_K = 2m$, and that $2m\theta_{S,K/k} \in \mathbb{Z}[G]$ as predicted by (11.18).

Back to the general case. Let $\mathbb{P}$ denote the set of all places in K, and let $\mathbb{P}_\infty$ be its subset of infinite places. Then the subgroup

$$K^o = \{\alpha \in K^\times : |\alpha|_v = 1 \text{ for all } v \in \mathbb{P}_\infty\} \tag{11.19}$$

is called the group of *anti-units* (the group of units E_K is defined by replacing $\mathbb{P}_\infty$ in (11.19) with $\mathbb{P}\backslash\mathbb{P}_\infty$; this explains the 'anti'). It follows from Kronecker's Lemma (see Exercise 11.1) that, for anti-units α, an ideal (α) determines α up to a root of unity in W_K. This observation guarantees that the following conjecture makes sense:

The Brumer-Stark Conjecture

Let K/k be an abelian extension of number fields. Then for each ideal $\mathfrak{a}$ in K there is an $\alpha \in K^o$ such that $\mathfrak{a}^{w\cdot\theta_{S,K/k}} = (\alpha)$, and such that the extension $K(\sqrt[w]{\alpha})/k$ is abelian.

In fact, α is determined up to a factor $\zeta \in W_K$, and $K(\sqrt[w]{\alpha})/k$ is abelian if and only if $K(\sqrt[w]{\zeta\alpha})/k$ is (since $K(\sqrt[w]{\zeta})/k$ is abelian, $K(\sqrt[w]{\alpha})/k$ is abelian if and only if $K(\sqrt[w]{\alpha}, \sqrt[w]{\zeta})/k$ is).

If K is a cyclotomic extension of $\mathbb{Q}$, the Brumer-Stark conjecture follows from Stickelberger's theorem (see Exercise 11.18). The fact that the Brumer-Stark elements give rise to abelian extensions of number fields k made Stark look more closely at what is happening here; see Tate's book [Ta1]. Recently, the Stark conjectures have been used to find explicit generators for certain Hilbert class fields by e.g. H. Bauer [Bau], Dummit & Hayes [DuH], Dummit, Sands & Tangedal [DST] and Roblot [Ro1, Ro2].

Amazingly, the Brumer-Stark theory can be generalized yet further: for abelian extensions K/k, define elements

$$\theta_n(K/k) = \sum_{\sigma \in G} \zeta_K(\sigma, -n)\sigma^{-1}.$$

Clearly $\theta_0(K/k)$ is the Brumer-Stark element for K/k. Let $w_n(K)$ be the maximal integer m such that $\mathrm{Gal}\,(K(\zeta_m)/K)$ has exponent dividing n; in particular, we have $w_1(K) = w = \#W_K$. Again it follows from the work of Deligne and Ribet that

$$w_n(K)\theta_n(K/k) \in \mathbb{Z}[G].$$

Coates [Co2] has shown that their results even imply that the elements

$$(N\mathfrak{a}^{n+1} - (\mathfrak{a}, K/k))\theta_n(K/k) \tag{11.20}$$

are integral. This allows us to define the n-th Stickelberger ideal $I_n(K/k)$ as the $\mathbb{Z}[G]$-ideal generated by elements in (11.20), as was suggested by Brumer (see Rideout's thesis [Rid]). Stickelberger's theorem (combined with Lemma 11.13) says that the ideal $I_0(K/\mathbb{Q})$ annihilates $\mathrm{Cl}\,(K)$. What do the $I_n(K/\mathbb{Q})$ annihilate?

Note that $\mathrm{Cl}\,(K)$ can be interpreted as the reduced K-group $\widetilde{K}_0(\mathcal{O}_K)$; it is also known that Milnor's $K_2(\mathcal{O}_K)$ is a finite group, and it can be shown that $I_1(K/\mathbb{Q})$ kills $K_2(\mathcal{O}_K)$, except perhaps for the 2-part. The conjecture of Birch & Tate (see Birch [54] for its origin) predicts that, for K totally real, $\#K_2(\mathcal{O}_K)$ equals $w_2(K) \cdot |\zeta_K(-1)|$. In general, it is expected that $I_n(K/\mathbb{Q})$ annihilates Quillen's K-groups $K_{2n}(\mathcal{O}_K)$.

Iwasawa Theory

One of the origins of Iwasawa theory is the construction of functions that interpolate zeta functions p-adically. In fact, since Hurwitz's ζ-function assumes rational values at the negative integers, it is tempting to ask whether there exists a continuous function defined on $\mathbb{Z}_p$ that takes the same values there, at least up to some trivial factors. The answer is yes, as was shown by

Leopoldt and Kubota (who constructed p-adic L-functions this way) as well as Iwasawa (who used p-adic integration). These p-adic L-functions can be used to show that, for large enough $n \in \mathbb{N}$, the p-class number h_n of $\mathbb{Q}(\zeta_{p^n})$ is given by

$$h_n = \# A_n = p^t, \quad t = \mu p^n + \lambda n + \nu; \tag{11.21}$$

here $\mu, \lambda, \nu \in \mathbb{N}_0$ are integers depending only on the prime p.

Later Iwasawa could prove a similar formula for p-class numbers in arbitrary $\mathbb{Z}_p$-extensions; these are infinite abelian extensions k_∞/k of a number field k with Galois group $\mathrm{Gal}\,(k_\infty/k) \simeq \mathbb{Z}_p$. A famous result of Ferrero and Washington says that $\mu = 0$ for every abelian extension $F/\mathbb{Q}$. A notoriously difficult question is whether $\mu = \lambda = 0$ for all totally real number fields F; this conjecture of Greenberg has only been verified in special cases. The number of independent $\mathbb{Z}_p$-extensions of a given number field k is at most $r_2 + 1$ (where r_2 denotes the number of complex primes of k), with equality if Leopoldt's conjecture on p-adic regulators is true.

Iwasawa also found a way to reinterpret p-adic L-functions in terms of his theory of $\mathbb{Z}_p$-extensions; this led to a very natural conjecture on the nature of these functions: the "Main Conjecture" of Iwasawa theory. See Nekovar [Nek].

Mazur and Wiles

This Main Conjecture soon occupied a central part of the research in Iwasawa theory, and when Mazur and Wiles eventually proved it in 1984, it was already known that it had quite a few important corollaries. For example, R. Greenberg had by then deduced the following conjecture of G. Gras from the Main Conjecture: Let K be an abelian extension of $\mathbb{Q}$ with conductor m, $L = \mathbb{Q}(\zeta_m)$, and put $G = \mathrm{Gal}\,(K/\mathbb{Q})$. The units in $E = E_K$ that can be written as products or quotients of elements of the form $\pm N_{L/K} \prod_a (1 - \zeta_m^a)$ form a group

$$C \;=\; C_K \;=\; \big\langle \pm N_{L/K}\big(\zeta_m^j \prod_a (1 - \zeta_m^a)\big)\big\rangle \cap E_K \tag{11.22}$$

called the group of *cyclotomic* (sometimes also called *circular*) units of K; note, however, that there are even more definitions of cyclotomic units than of Stickelberger ideals floating around.

Gras conjectured that, for even characters $\chi \in G\widehat{\ }$, the components $\mathrm{Cl}_p(\chi)$ and $(E/C)_p(\chi)$ not only should have the same order, but that they are isomorphic as $\mathbb{Z}_p[G]$-modules. Thanks to Mazur and Wiles, this is now a theorem.

Another corollary of the Main conjecture is a class number formula conjectured by Iwasawa and Leopoldt. In order to formulate it, let us write $a \sim b$ for p-adic integers $a, b \in \mathbb{Z}_p$ when a and b are divisible by the same p-power.

Theorem 11.28. *Let $F/\mathbb{Q}$ be an abelian extension with Galois group G, and assume that p is an odd prime not dividing $(F : \mathbb{Q})$. Let $\chi \neq \omega$ be an odd character of* $\mathrm{Gal}\,(F/\mathbb{Q})$*; then*

$$\#\mathrm{Cl}_p(F)(\chi) \ \sim \ B^g_{1,\chi^{-1}}. \tag{11.23}$$

Here $g = (\mathbb{Q}_p(\chi) : \mathbb{Q}_p)$, where $\mathbb{Q}_p(\chi)$ is the smallest extension of $\mathbb{Q}_p$ containing the values of χ. □

The condition that $p \nmid (F : \mathbb{Q})$ was removed later by D.R. Solomon [Sol].

As an example, take $F = \mathbb{Q}(\zeta_p)$; here $G \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, hence χ takes values in $\mu_{p-1} \subset \mathbb{Q}_p$, and we have $g = 1$. Theorem 11.28 says that if i is odd then $\#\,\mathrm{Cl}_p(F)(\omega^i) \sim B_{1,\omega^{-i}}$, congruence (11.14) says that $B_{1,\omega^{-i}} \equiv \frac{1}{p-i}B_{p-i} \bmod p$, hence we find that $\mathrm{Cl}_p(F)(\omega^i) \neq 1$ if and only if $p \mid B_{p-i}$; this is of course the theorem of Herbrand–Ribet.

In a similar way we can explain (and improve on) the results of Gut and Kleboth: take $F = \mathbb{Q}(\zeta_{4p})$; its characters are either characters χ belonging to $K = \mathbb{Q}(\zeta_p)$, or they have the form $\psi\chi$, where ψ is the nontrivial Dirichlet character modulo 4. The relative class group $\mathrm{Cl}_p(F/K)$ corresponds to characters $\psi\chi$, that is, $\mathrm{Cl}_p(F/K) \simeq \bigoplus_\chi \mathrm{Cl}_p(F)(\psi\chi)$, and $\mathrm{Cl}_p(K) \simeq \bigoplus_\chi \mathrm{Cl}_p(F)(\chi)$. Since ψ is an odd character, $\psi\omega^i$ is odd if and only if i is even; for such values of i we find that $\#\,\mathrm{Cl}_p(F)(\psi\omega^i) \sim B_{1,\psi\omega^{-i}}$ by (11.23), and $B_{1,\psi\omega^{-i}} \equiv \frac{1}{p-i}B_{p-i}(\psi) \bmod p$ by (11.14). Finally $\frac{1}{p-i}B_{p-i}(\psi) \sim E_{p-1-i}$ by the definition of Euler numbers, hence we find that for even integers $i \leq p$, the component $\mathrm{Cl}_p(F)(\psi\omega^i)$ is nontrivial if and only if $p \mid E_{p-1-i}$.

Yet another consequence of the Main Conjecture ([MW, Thm. 5]) due to Coates [Co1] is the formula $\#K_2(\mathcal{O}_K) = w_2(K) \cdot |\zeta_K(-1)| \cdot 2^a$ for real abelian extensions $K/\mathbb{Q}$ and some 2-power 2^a, that is, the truth of the Birch-Tate conjecture up to 2-powers. The problem with the 2-part came from the fact that Iwasawa's Main Conjecture was usually formulated only for odd primes p; the analogous conjecture for $p = 2$ was stated by Iwasawa (see Federer [Fe]), Kolster [Kol] showed that it would imply the 2-primary part of the Birch-Tate conjecture, and finally Wiles [Wil] proved the Main Conjecture also for $p = 2$. For a proof using the simpler methods described in the next subsection, see Greither [Gre].

The connection between K-groups and the class groups of cyclotomic fields is much stronger than indicated by this last result. In fact, Kurihara [Kur] showed that Vandiver's conjecture would follow from conjectures about the structure of Quillen's K-groups $K_n(\mathbb{Z})$; he exploits this relationship to construct a surjection $K_4(\mathbb{Z}) \otimes \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{C}_{p-3}$, where $\mathcal{C}_{p-3} = \mathrm{Cl}_p(F)(\omega^{p-3})$, and then shows that $K_4(\mathbb{Z})$ is small enough to enforce $\mathcal{C}_{p-3} = 0$ (in fact, today we know that $K_4(\mathbb{Z}) = 0$). A more general result in this direction is due to Soulé [Sou]; see Ghate [Gha] for an introduction.

Thaine, Kolyvagin and Rubin

Stickelberger's relation contains no information on the class group of real abelian fields (see Exercise 11.18, for example). In [Tha], Thaine used cyclotomic units to construct annihilators of ideal class groups of real abelian fields F: let $m = \operatorname{cond} F$ be the conductor of F, $G = \operatorname{Gal}(F/\mathbb{Q})$ its Galois group, put $K = \mathbb{Q}(\zeta_m)$, and define the subgroup $C_F \subseteq E_F$ of cyclotomic units as in (11.22) above. Then Thaine proved that for any prime p not dividing $(F : \mathbb{Q})$, 2θ kills $\mathrm{Cl}_p(F)$ whenever $\theta \in \mathbb{Z}[G]$ kills the p-Sylow subgroup of E_F/C_F.

By refining Thaine's construction, Kolyvagin could not only give an elementary proof of Gras' conjecture but also of Ribet's converse of Herbrand's theorem. Rubin finally showed how Kolyvagin's theory of Euler systems could be applied to prove the main conjecture of Iwasawa theory; see e.g. his appendix in Lang's [La2], [Ru1], or the survey [PR] by Perrin-Riou. All this is explained beautifully in the second edition of Washington's book [Was1]. Rubin has written a book on Euler systems that will be published soon. His CIME lectures [CGR] on this topic have just appeared.

Notes

Normal Integral Bases

It was not completely accurate when we said that our proof of Eisenstein's reciprocity law would follow Hilbert's arguments as laid out in his Zahlbericht [368]: in fact we left out all of his results on normal integral bases of number fields, because they are not needed for deriving Eisenstein's reciprocity law. We cannot disregard them completely, however, because these results moved to the center of mathematical interest during the 1970's. This was due to the completely unexpected connections with Artin's L-series; in order to see what has happened we have to go back to Hilbert's Zahlbericht.

In Chapter 3 we have seen that, for odd primes p, all subfields of $\mathbb{Q}(\zeta_p)$ have a normal integral basis. More generally, Hilbert showed

Theorem 11.29. (Satz 132) *Let $K/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ such that $(\operatorname{disc} K, (K : \mathbb{Q})) = 1$. Then $\mathcal{O}_K$ has a NIB.* □

Hilbert's proof was quite simple: he used the theorem of Kronecker and Weber to embed K in some $L = \mathbb{Q}(\zeta_m)$ and applied Proposition 3.6 to reduce the problem to finding a NIB of $\mathcal{O}_L$, which is easy.

Now where are the Gauss sums? Take odd primes p, ℓ with $p \equiv 1 \bmod \ell$, and let k denote the subfield of degree ℓ in $\mathbb{Q}(\zeta_p)$. Since $\operatorname{disc} k = p^{\ell-1}$, $k/\mathbb{Q}$ satisfies the hypothesis of Satz 132 and thus has a NIB generated by $\nu \in \mathcal{O}_k$ (this means that a NIB is given by $\{\nu, \nu^\sigma, \ldots, \nu^{\sigma^{\ell-1}}\}$, where σ is a generator of $G = \operatorname{Gal}(k/\mathbb{Q})$. In this situation, the element

$$\Omega \ = \ \nu + \zeta_\ell \nu^\sigma + \zeta_\ell^2 \nu^{\sigma^2} + \ldots + \zeta_\ell^{\ell-1} \nu^{\sigma^{\ell-1}} \in \mathbb{Z}[\zeta_p]$$

is called a *root number* (Wurzelzahl) of k by Hilbert. The principal properties of root numbers are given by

Theorem 11.30. (Satz 133) *Let σ be the $\mathbb{Q}$-automorphism of $K = \mathbb{Q}(\zeta_\ell)$ defined by $\zeta_\ell \longmapsto \zeta_\ell^r$, where r is a primitive root modulo ℓ, and let k be as above. Then root numbers of k have the following properties:*

i) $\omega := \Omega^\ell \in \mathcal{O}_K$*, and* $\omega^{\sigma - r}$ *is an ℓ-th power in* $K^\times$*.*
ii) $\Omega \equiv \pm 1 \bmod (1 - \zeta_\ell)$*, and* $\omega \equiv \pm 1 \bmod (1 - \zeta_\ell)^\ell$*.*
iii) $N_{K/\mathbb{Q}} \omega = p^{\ell(\ell-1)/2}$*.*
iv) $\omega \in K^\times \setminus K^{\times \ell}$*.* □

As a matter of fact, Hilbert neither states nor proves property iv), but when he claims that properties i), ii) and iii) suffice to characterize root numbers, he makes use of it:

Theorem 11.31. (Satz 134) *If $\omega \in \mathcal{O}_K$ satisfies the properties i) – iv) in Theorem 11.30, then $\Omega = \sqrt[\ell]{\omega}$ is a root number of k.* □

Next Hilbert studies the prime ideal decompositions of root numbers with the techniques discussed in Section 11.1 (this is no problem: the essential property is that root numbers as well as Gauss sums generate *abelian* extensions).

We still haven't seen any Gauss sums, but now they enter the picture: since $\mathbb{Q}(\zeta_p)$ has a NIB, so does k (its subfield of degree ℓ), and the proof of Proposition 3.6 shows that we can take

$$\begin{aligned}
\lambda_0 &= \zeta_p + \zeta_p^{R^\ell} + \ldots + \zeta_p^{R^{(m-1)\ell}} \\
\lambda_1 &= \zeta_p^{R} + \zeta_p^{R^\ell + 1} + \ldots + \zeta_p^{R^{(m-1)\ell + \ell}} \\
&\ldots \\
\lambda_{\ell-1} &= \zeta_p^{R^\ell - 1} + \zeta_p^{R^{2\ell} - 1} + \ldots + \zeta_p^{R^{m\ell - 1}}
\end{aligned}$$

as a NIB for k, where R is a primitive root modulo p. Hilbert calls the corresponding root number $\Lambda = \Omega$ a Lagrangian root number *(Lagrange'sche Wurzelzahl)*; but $\Lambda = \sum_{j=0}^{p-2} \zeta_\ell^j \zeta_p^{R^j}$ is nothing but the Gauss sum for the character χ over $\mathbb{F}_p$ that maps $R^j \bmod p$ to ζ_ℓ^j. In particular, Hilbert's results on root numbers apply to Gauss sums.

Back to normal integral bases. Speiser [Sp] later observed that Hilbert's condition $(\operatorname{disc} K, (K : \mathbb{Q})) = 1$ could be weakened; he found

Theorem 11.32. *If $K/\mathbb{Q}$ is a normal extension such that $\mathcal{O}_K$ has a NIB, then the ramification index of each prime does not divide $(K : \mathbb{Q})$ i.e., $K/\mathbb{Q}$ is tamely ramified. Moreover, if $K/\mathbb{Q}$ is abelian, this condition is sufficient.*

This is not so hard to prove: recall from Hilbert's work that if K has a NIB generated by α, then k has a NIB generated by $\operatorname{Tr}_{K/k}\alpha$. In particular, the existence of a NIB for K implies that $\operatorname{Tr}_{K/k}\mathcal{O}_K = \mathcal{O}_k$. Now it is easy to see that a prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ divides $\operatorname{Tr}_{K/k}\mathcal{O}_K$ if and only if $\mathfrak{p}$ is wildly ramified in K/k.

In 1932, E. Noether [Noe] looked at this problem from the viewpoint of the local-global principle and showed that Speiser's condition $e(p) \nmid (K : \mathbb{Q})$ was equivalent to the existence of a local NIB, i.e. if $K/\mathbb{Q}$ is normal, then p is tamely ramified in $K/\mathbb{Q}$ if and only if $\mathcal{O}_\mathfrak{p}$ has a NIB, where $\mathcal{O}_\mathfrak{p}$ is the integral closure of the completion $K_\mathfrak{p}$ of K at some prime ideal $\mathfrak{p}$ above p (see Chapman [Ch1] for a simple proof).

There are two obvious ways to generalize these results of Hilbert, Speiser and Noether: one can replace $\mathbb{Q}$ by a general number field (the naive way of doing this does not work at all: see Exercise 11.31 for a simple counterexample. In fact, Greither, Replogle, Rubin & Srivastav [GRR] have recently shown that $\mathbb{Q}$ is the only number field such that all tame abelian extensions have a normal integral basis), and one can look at non-abelian extensions of $\mathbb{Q}$. In the last direction we have the following result of Martinet [Ma1]:

Proposition 11.33. *If $K/\mathbb{Q}$ is a tame normal extension with Galois group $Gal(K/\mathbb{Q}) \simeq D_p$ (dihedral group of order $2p$), then $K/\mathbb{Q}$ has a NIB.*

The next simplest non-abelian groups are the quaternion groups. Here Martinet [Ma2] found:

Proposition 11.34. *There exist tame normal extensions $K/\mathbb{Q}$ with Galois group isomorphic to H_8 (the quaternion group of order 8) which do (or do not) possess a NIB.*

Now H_8 has a unique irreducible character χ of degree 2. Artin showed how to attach an L-series $L(s,\chi)$ to the pair K and χ; the corresponding function $\Lambda(s,\chi)$ (obtained by multiplying $L(s,\chi)$ by appropriate Γ-factors as in Section 10.4) satisfies a functional equation of type $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\overline{\chi})$, where $W(\chi)$ is a root of unity called the *Artin root number* of χ; it follows from the functional equation that $W(\chi) = \pm 1$ for real-valued characters χ. Fröhlich & Queyrut [FQ] showed that $W(\chi) = +1$ whenever χ is the character of a real representation. On the other hand, Armitage showed that, for the irreducible 2-dimensional character of H_8, the root number does assume negative values. This led Serre to the 'crazy idea' that the value of $W(\chi)$ might be connected with the existence of a NIB, and in fact, Fröhlich eventually managed to prove

Theorem 11.35. *Let $L/\mathbb{Q}$ be a tame normal extension with $Gal(K/\mathbb{Q}) \simeq H_8$. Then $L/\mathbb{Q}$ has a NIB if and only if $W(\chi) = 1$.*

It can be shown that $W(\chi) = 1$ is also equivalent to $L(1/2,\chi) = 0$. See the Notes in Narkiewicz [Nar, Chapter 4] for more.

There is (in some sense) a final answer which was given by M. J. Taylor (by now, of course, the whole area has been generalized – at least conjecturally – almost beyond recognition by Chinburg, Fröhlich, M.J. Taylor, and others):

Theorem 11.36. *Let $L/\mathbb{Q}$ be a tame normal extension with $Gal(K/\mathbb{Q}) = G$. If G has no symplectic characters, then $L/\mathbb{Q}$ has a NIB. If G has a symplectic character, then $\mathcal{O}_L$ or $\mathcal{O}_L \oplus \mathcal{O}_L$ is a free $\mathbb{Z}[G]$-module.*

A symplectic character of a finite group G is a character corresponding to a representation of G that factorizes through the symplectic group $\mathrm{Sp}_{2n}(\mathbb{C})$. Note that abelian groups or groups of odd order do not possess symplectic characters, but that H_8 does. For a leisurely introduction to this area, see Erez [Ere]; the real stuff is in Fröhlich [Fr1]. For connections between NIB's, Gauss sums and Leopoldt's Spiegelungssatz see Brinkhuis [Br2, Br3].

The Stickelberger Relation

Theorem 11.4 was already known to Cauchy, Jacobi, Eisenstein, and Kummer. Of course, they had to use a different language since ideals had not yet been invented then. Jacobi's substitute for Gauss sums were the polynomials

$$F(x, \alpha) = x + \alpha x^{g_1} + \ldots + \alpha^{p-2} x^{g_{p-2}},$$

where x is an indeterminate, α a complex number with $\alpha^{p-1} = 1$, and where the exponents g_j are defined by $g_j \equiv g^j \bmod p$, $0 \le g_j \le p-1$, with g a primitive root modulo p. It is clear that substituting $x = \zeta_p$ gives $F(\alpha) := F(\zeta_p, \alpha) = -G(\chi)$, where χ is the character modulo p of order $p-1$ defined by $\chi(g) = \alpha$. Thus the relation $G(\chi)G(\chi^{-1}) = \chi(-1)p$ translates into $F(x,\alpha)F(x,\alpha^{-1}) = \alpha^{(p-1)/2}(p - 1 - x - \ldots - x^{p-1})$. Jacobi also shows that $F(\alpha^a)F(\alpha^b) = \psi_{a,b}(\alpha)F(\alpha^{a+b})$ as long as α^a, α^b and α^{a+b} are different from 1, and that $\psi_{a,b}(\alpha) \in \mathbb{Z}[\alpha]$: of course $\psi_{a,b}(\alpha) = -J(\chi^a, \chi^b)$ is a Jacobi sum. He then replaces α by g and shows that the congruence $\psi_{a,b}(g) \equiv -\frac{(a+b)!}{a!b!} \bmod p$ holds (this is how Cauchy and Jacobi could determine the "prime ideal factorization" of Jacobi sums without having the notion of ideal numbers, let alone ideals). This is of course just the congruence (11.12): in fact, we have $n = 1$ since $m = p - 1$, and if we write $\mathcal{P} = (1 - \zeta_p, g - \alpha)$, then the congruence is valid modulo $\mathcal{P}$. Replacing α by g turns the Jacobi sum on the left hand side into $\psi_{a,b}(g)$, and the resulting congruence is not only valid modulo $(1 - \zeta_p)$ but modulo p since both sides are elements of $\mathbb{Z}$.

Next Jacobi compares the equality $\psi_{a,b}(\alpha) = \frac{F(\alpha^a)F(\alpha^b)}{F(\alpha^{a+b})}$ with the congruence $\psi_{a,b}(g) \equiv -\frac{(a+b)!}{a!b!} \bmod p$ and concludes that $F(\alpha^a)$ seems to behave very much like $-\frac{1}{a!} \bmod p$. He then goes on to prove a special case of Stickelberger's congruence.

Cauchy's work is somewhat hard to read (the motto 'more Landau, less Goethe!' would have stood him in good stead). His main work [123] on cyclotomy has about as many pages as this book. The basic relations for Gauss sums are all there, but scattered throughout his treatise. The multiplication formula $G(\chi_1)G(\chi_2) = J(\chi_1,\chi_2)G(\chi_1\chi_2)$ for Gauss sums occurs as (9) on p. 7, and the relations $G(\chi)G(\chi^{-1}) = \chi(-1)p$, $J(\chi,\chi)\overline{J(\chi,\chi)} = p$ as well as $G(\chi)^2 = p^*$ for the quadratic character χ on $\mathbb{F}_p^\times$ can be found on pp. 92–93. On p. 15, he gives $4p^\mu = x^2 + ny^2$, where $n \equiv 3 \bmod 4$, and on p. 18 he shows that μ is congruent to the smallest integer $\equiv \pm 2B_{(n+1)/4} \bmod p$. On p. 106, he discusses a similar result for $n \equiv 1 \bmod 4$. The last chapters are dedicated to congruences for binomial coefficients: on p. 410, he gives Gauss's result that $x \equiv \binom{2n}{n} \bmod p$ for $p = 3n+1 = x^2+3y^2$, and on the next 15 pages he discusses analogous results with 3 replaced by other primes $\equiv 3 \bmod 4$ up to $p = 43$.

The general congruence 11.10 is due to Stickelberger [759]; for different proofs, see Brinkhuis [Br1], Coates [Co2], Conrad [Con], Gillard [Gil], Gras [Gra], Joly [413], and Mertens [581]. There are also various textbooks containing proofs of Stickelberger's relation: see e.g. Ireland & Rosen [386], Lang [La1, La2], Moreno [Mo1], and Washington [Was1]. The very simple proof we have given is taken from Gras [Gra] (it coincides essentially with Lang's presentations). The proof of Davenport & Hasse [DaH] is presented in the book [386] of Ireland & Rosen. See also Fröhlich [Fr2], Ibrahimoglu [Ibr] and Washington [Was2] for proofs of Stickelberger's theorem.

Why Hilbert did not mention Stickelberger's general relation in his Zahlbericht is quite mysterious; Davenport rediscovered Stickelberger's contribution in 1934 after he and Hasse had given a new proof of the relation. Three months after Davenport's discovery, Hasse [Has2] writes

> I found this proof very nice indeed, and much simpler than I expected from my first scanning of Stickelberger's paper.

It is conceivable that Hilbert's first impression was similar.

Schwering [Sch] proved that Jacobi sums for characters of odd prime order $\ell > 3$ are congruent to 1 mod $(1-\zeta_\ell)^3$; this is sharper than the congruence in Lemma 11.6.vi).

A drastic improvement of the Stickelberger congruence is due to Gross & Koblitz [GK], who gave precise p-adic expressions for Gauss sums that contain Stickelberger's result as a very special case. Washio, Shimaura, & Shiratani derive a congruence following from the Gross-Koblitz formula from Stickelberger's congruence. See also Koblitz [Kob] (an excellent book providing a lot of insight, but requiring quite some background at various places), and Lang [La2] for a more elementary treatment.

A completely new approach to the Stickelberger relation using the arithmetic of the Jacobian variety of the curve $y^2 = 1 - x^l$, where l is an odd prime, was presented by Shimura and Taniyama in [ST, p. 129]; see also Kubota [Kub].

Eisenstein's Reciprocity Law

Eisenstein's reciprocity law for residues of ℓ-th powers is due to Eisenstein [204] himself. He published his proof in 1850, using Kummer's language of ideal numbers. Jacobi had claimed in 1839 (see [403]) to be in possession of this law in the special cases $n = 5$, 8 and 12, but never published anything on them. In [400, p. 263], he writes

> Mit den Resten der 8^{ten} und 5^{ten} Potenzen, welche ganz neue Principien nöthig machen, bin ich ziemlich weit vorgerückt; sobald ich den betreffenden Reciprocitätsgesetzen die wünschenswerthe Vollendung gegeben habe, werde ich sie der Akademie mittheilen.[3]

Whether Jacobi knew that the corresponding rings $\mathbb{Z}[\zeta_5]$ and $\mathbb{Z}[\zeta_8]$ are Euclidean is questionable: in his lectures, the Euclidean algorithm is not used to prove unique factorization (in fact, this problem is not addressed at all) but to the problem of computing power residue symbols using reciprocity! In a letter to Jacobi, Hermite [Hrt] showed in 1845 that $\mathbb{Z}[\zeta_p]$ is a principal ideal ring for $p = 5$ and $p = 7$ by a different method. Whatever the reasons, Jacobi did not publish anything on this. Even when Reuschle wrote to Jacobi on Nov. 11, 1846 and asked him for criteria for $(10/p)_n$ for $n = 5, 7, 8, 9$ (he was computing the period length of decimal fractions for a table he was compiling: see Hertzer [365]), Jacobi's answer from Dec. 13, 1846 (published by Lampe [475]) contains criteria for $(10/p)_8$ plus the rather shallow remark that criteria for $(10/p)_5$ would depend on the factorization of p in $\mathbb{Z}[\zeta_5]$.

Eisenstein seems to have rediscovered these special cases in 1844, as his letter to Stern (probably July 1844) shows:

> Die Reste der 8ten, 12ten und auch der 5ten Potenzen, welche fertig sind, arbeite ich jetzt aus. Das ist ein Feld, auf dem ich mich ganz frei bewegen kann, denn hier hat selbst Jacobi nichts, wie er mir gesteht.[4]

At that time, Eisenstein visited Jacobi weekly, and Jacobi's accusation of plagiarism lay two years ahead.

Apart from the allusions by Jacobi and Eisenstein, the first contribution to quintic residuacity is due to Pépin [635], who used an approach via Jacobi sums. Later, L. Tanner hit upon results on quintic power residues without recognizing them as such (he was studying the coefficients of quintic Jacobi sums); Tanner's results were explained by E. Lehmer in [500].

Hilbert's proof of Eisenstein's reciprocity law in Section 11.2 can be simplified somewhat by using Theorem 11.12; see Ireland & Rosen [386]. For

[3] I have advanced considerably the theory of the 8th and 5th power residues which require completely new principles. As soon as I have given these reciprocity laws the desired perfection, I will communicate them to the academy.

[4] I am now elaborating the residues of the 8th, 12th and also the 5th powers, which are completed. This is an area where I can move freely, as even Jacobi admits not to have anything on them.

other (but similar) proofs, see Landau [Lan], Spearman & Williams [745], as well as Weil's beautiful paper [827].

The generalization to ℓ^2-th powers was sketched by Furtwängler in [255], and the law for ℓ^ν-th powers was proved by Hasse. In the case $\ell = 2$, Hasse could only prove the reciprocity law for $2^{\nu-2}$-th powers in $\mathbb{Q}(\zeta_{\ell^\nu})$. Here is his result for odd prime powers:

Theorem 11.37. *Let $m = \ell^n$ be an odd prime power. Assume that $a \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[\zeta_m]$ be relatively prime; if $\alpha \equiv \xi^\ell \bmod (1-\zeta_m)^2$ and $a^{\ell-1} \equiv 1 \bmod m$, then*

$$\left(\frac{a}{\alpha}\right)_m = \left(\frac{\alpha}{a}\right)_m.$$

Apparently Hasse, at the time of writing [336], was not aware of the papers of Western [837, 838] which contain stronger results and simpler proofs; Western's discussion of primary elements is not very clear, but fortunately Berndt, Evans & K.S. Williams gave a readable and simplified account of Western's paper in their excellent book [48]. Nevertheless, an explicit definition of primariness in Western's sense is still a desideratum. Bohnicek claims in [63] that [62] contains a proof for Hilbert's n-th power reciprocity law for number fields K in which Eisenstein's n-th power reciprocity holds; unfortunately, [62] was unaccessible to me. Takagi [790] proves Eisenstein's reciprocity law for ℓ-th powers in arbitrary number fields containing ζ_ℓ. Wojcik [873] gives a version of Eisenstein's reciprocity law for n-th powers based on yet another definition of primary integers; since the special case $n = 2$ of his law is an incorrect formulation of the quadratic reciprocity law, his proof (which is based on his results from [874]) needs to be checked. It seems that a definitive treatment of Eisenstein's reciprocity law for n-th powers is still lacking. For an application of Eisenstein's reciprocity law to n-th powers of integers (this problem was discussed in the Notes of Chapter 4) see Kraft & Rosen [436]. Hayes [Hay2] uses Eisenstein's reciprocity law for computing conductors of what he calls Eisenstein characters; in [Hay1] he proved an analogue of Eisenstein's reciprocity law in function fields.

Class Numbers

The integrality of $h = \frac{R-N}{d}$ (Lemma 11.15) was proved by Cauchy [Cau] and Stickelberger [759]. The proof given here is Stickelberger's, which is much simpler than the one in Hasse's book [342]. Hasse also proved the integrality of the minus class number h_p^- in Equation (11.15) (see [Has1]). Cauchy noticed the connections with Bernoulli numbers; see also Voronoi [Vor]. For some slick proofs of congruences between Bernoulli numbers (originally due to Kummer and Voronoi), see Johnson's article [Joh]. For generalizations of many results about Bernoulli numbers to generalized Bernoulli numbers, see Ernvall [Er1].

Computation of cyclotomic invariants (that is, irregular primes, irregularity index, Iwasawa invariants etc.) continues despite the proof of Fermat's last theorem; for the latest results, see Buhler, Crandall, Ernvall, Metsänkylä, & Shokrollahi [BC1, BC2].

Special cases of Proposition 11.16 were already known to Cauchy and Jacobi; since they only had Gauss sums over $\mathbb{F}_p$ at their disposal, all they could treat were primes $p \equiv 1 \bmod d$. Jacobi even restricted to prime values $d = -\ell$, but conjectured that $\frac{N-R}{\ell}$ always equals the class number of $\mathbb{Q}(\sqrt{-\ell}\,)$ [Jac]. Cauchy and Jacobi published their results at about the same time (shortly after Jacobi's visit in Paris in 1829), but apparently they have been written independently (the same remark applies to Cauchy's and Jacobi's versions of Gauss's sixth proof of quadratic reciprocity that we were talking about in the Notes of Chapter 8). The extension of these results to primes not necessarily of the form $p \equiv 1 \bmod \ell$ was accomplished by Stickelberger [759]. Hilbert's Zahlbericht [368] only gives the part due to Cauchy and Jacobi, as does e.g. the exposition in Ireland & Rosen [386]. A proof of the general result along these lines borrowing ideas from the paper of Coates [Co2] is given in Exercise 11.8. Mitchell [Mi1, Mi2] showed, using Jacobi sums, that the minus class number of the subfield $K \subseteq \mathbb{Q}(\zeta_p)$ of degree e annihilate certain parts of the minus class group of K. MacKenzie [McK] derives relations in the class group of $\mathbb{Q}(\zeta_n)$ that seem to come from the fact that Jacobi sums are principal; his proof, however, uses Fourier transforms, and it would be desirable to see if his method can be used to find the prime ideal factorization of Jacobi sums.

Euler numbers were first studied by Euler in 1755; they satisfy the relation

$$\sum_{\nu=0}^{m} \binom{2m}{2\nu} E_{2\nu} = 0$$

for $m \geq 1$, and this implies that Euler numbers are integral; the first few values are $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, $E_8 = 1385$. Their connection with class groups of $\mathbb{Q}(\zeta_{4m})$ was studied by Gut [Gut] and Ernvall & Metsänkylä [EM]. For a survey of known results see Salié [Sal].

The index of the Stickelberger ideal (Theorem 11.25) was computed by Iwasawa, who also seems responsible for introducing the Stickelberger ideal itself (of course Kummer and Stickelberger never talked about ideals in group rings). Our calculation of $(R^- : I^-)$ is based on an unpublished (but weblished) manuscript by Robin Chapman [Ch2] and is close in spirit to the one given by Lang [La2]. The treatment in Washington [Was1] is closer to the original computation by Iwasawa. Jha [Jha] wrote a survey on class number formulas and Stickelberger ideals, and so did Kimura [Kim]; Kimura's book seems to be the better choice but unfortunately it is written in Japanese.

For surveys on Iwasawa theory, the main conjecture, Euler systems etc. we refer the reader to Coates [Co3] (he also discusses relevant work of Kubert & Lang on the occurrence of the Stickelberger ideal in the theory of cusps of modular forms), Lang [La3], Nekovar [Nek], Rubin [Ru1, Ru2] and Tamme [Ta] as well as to the books on cyclotomic fields by Lang [La2] and Washington [Was1].

Fermat's Last Theorem

The claim that the equation $x^3 + y^3 = z^3$ has only trivial solutions in integers was first claimed (with a completely inadequate proof) by al-Hogendi more than six centuries before Fermat: see Rashed [Ras] for more on this, as well as for other details about the contributions of Arabic mathematics to number theory.

Legendre included his results on Fermat's Last Theorem as a second supplement to his book on number theory; the first supplement was added in 1816, and the book was brought into its final form for the third edition in 1830. Legendre also studied the equation $x^3 + y^3 = az^3$ for $a \in \mathbb{N}$ and claimed that there are no non-trivial solutions if $a = 1, 2, 3, 4, 5, 6, 8, 16 \ldots$; Pépin noticed, however, that $17^3 + 37^3 = 6 \cdot 21^3$, as did Lucas in a letter to Sylvester as well as Dudeney in his booklet "The Canterbury Puzzles".

The results on Fermat's Last Theorem in Exercises 11.32 – 11.37 can all be found in Hasse's Zahlbericht [340] as well as in the third volume of Landau's Vorlesungen [Lan]. Frobenius [Fro] showed how the criteria of Wieferich and Mirimanoff could be extended to primes $q > 3$; using quite complicated computations, this has been done up to $q = 89$ by Granville & Monagan [GM] and then to $q = 113$ by J. Suzuki [Su]. Wieferich derived his result from a congruence due to Kummer; a simple proof of this congruence using Herbrand's theorem was given recently by Granville [Gr2].

For a proof of a result containing Exercise 11.35 see Wendt [Wen]; his method was taken up again by Fee & Granville [FG], as well as Lenstra & Stevenhagen [LeSt]; see also Helou [Hel]. Attempts at attacking the case of prime pairs p, $6p + 1$ are due to Granville [Gr1]. For other connections between reciprocity and Fermat's Last Theorem, see Bachmann [Ba], Delcour [154], Edwards [181], Furtwängler [254], Holzer [373], Noguès [Nog], Terjanian [Ter, 799], and Vandiver [812], as well as Ribenboim's excellent pre-Wiles classic [Ri1] and his article [Ri2].

After centuries of research on certain types of diophantine equations, it was eventually noticed that equations like $x^3 + y^3 = az^3$ or $z^2 = x^4 + y^4$ belong to the family of elliptic curves; in fact, Fermat's proof of FLT for $n = 4$ via infinite descent has been developed into an algorithm that allows us to compute the group of rational points for a large class of elliptic curves (unfortunately, the non-triviality of the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})$ complicates things considerably; Fermat and Euler were simply lucky that their curves had trivial Ш). Only the cases $n = 3, 4$ and 7 of Fermat's equation are known to lead to elliptic curves: $x^3 + y^3 = z^3$ is already elliptic and has the Weierstraß form $y^2 = x^3 - 432$, the quartic Fermat equation $x^4 + y^4 = z^4$ leads to the elliptic curve $z^2 = x^4 + y^4$ with Weierstraß form $y^2 = x^3 - 4x$ (see Exercise 10.17 for the analogous problem of $z^2 = x^4 - y^4$), and Lamé's solution of $x^7 + y^7 = z^7$ boils down to solving $u^2 = s^4 + 6s^2t^2 - \frac{1}{7}t^4$, which can also be written as $y^2 = x(x^2 - 3 \cdot 7^2 x + 2^4 \cdot 7^3)$; this is an elliptic curve of conductor 7^2 whose only rational points are its two torsion points. Since there are no elliptic curves of 5-power conductor, a similar proof for the case $n = 5$ of FLT probably doesn't exist. In this connection it is interesting to note that Chowla [Cho] has shown that the Fermat curve $x^p + y^p + z^p = 0$ has a nontrivial rational point if and only if the hyperelliptic curve $y^2 = 4x^p + 1$ does.

Hellegouarch associated the elliptic curve $E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$ to any solution a, b, c of $A^p + B^p = C^p$ in order to study torsion points on elliptic curves; Frey was the first to suggest that $E_{a,b,c}$ should have properties that are so weird that the curve cannot exist. After contributions of Serre, Ribet succeeded in proving that the conjecture of Taniyama-Shimura-Weil would imply FLT. Wiles, with a little help from R. Taylor, eventually managed to prove enough of this conjecture to be able to derive Fermat's Last Theorem. For an exposition of his proof plus an explanation of the terms used above, see the Boston Proceedings edited by Cornell, Silverman, & Stevens [CSS]. Remarkably, Stickelberger's congruence is still present there: look up Theorem 4.4.1. in Tate's contribution, where these congruences play a role in the classification of certain finite flat group schemes.

Other expositions of the proof of Fermat's Last Theorem (or, rather, of a large part of the Taniyama-Shimura conjecture) ordered approximately by level of difficulty are Cox [Cox], van der Poorten [vdP], Hellegouarch [Hll], J. Kramer [Kr1, Kr2], Moreno [Mo2], K. Murty [Mu1, Mu2], R. Murty [Mu], Schoof [Sf1, Sf2], Bertolini & Canuto [BC], Darmon [Dar], Ribet [Rb2], and Darmon, Diamond & R. Taylor [DDT]. Note that some of these surveys were written before the gap in Wiles' first proof was filled.

Exercises

11.1 Prove Kronecker's assertion that any algebraic integer $\alpha \in \mathcal{O}_K$ such that $|\alpha^\sigma| = 1$ for every embedding $\sigma : K \hookrightarrow \mathbb{C}$ is a root of unity. Give a counterexample in the case where α is not integral.

11.2 Prove Corollary 11.5.

11.3 (cf. Sharifi [731]) Generalize Exercises 6.5 and 7.12 to ℓth powers: for primes $p = \Phi_\ell(\ell x)$, show that any divisor a of x is an ℓ-th power residue modulo p. (Hint: observe that $p = N(1 - \ell x \zeta_\ell)$ and use Eisenstein's reciprocity law).

11.4 Let $p \equiv 1 \bmod 5$ be a prime, and $\pi \in \mathbb{Z}[\zeta_5]$ a semi-primary element of norm p. Let $\chi = (\,\cdot\,/\pi)$ be the quintic power residue character; then show that $J(\chi, \chi) = \pi\sigma_3(\pi)$, where σ_3 is the automorphism of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ mapping ζ_5 to ζ_5^3. How does multiplying π by the primary unit ε^2, where $\varepsilon = \frac{1}{2}(1 + \sqrt{5})$, influence the product $\pi\sigma_3(\pi)$? Show also that $J(\chi^2, \chi^2) = \pi\sigma_2(\pi)$, and use Proposition 4.27 to deduce that $(\pi/2) = (\pi/2)$.

11.5 Assume the notation of Proposition 11.2. Write $G(\chi^m) = \mathfrak{p}^\theta$, where $\theta = \sum_a b_a \sigma_a$. Use the facts that $\sum_a b_a = \frac{1}{2}\phi(m)m$ and that the Jacobi sums $J(\chi, \chi^t)$ are integral for $t = 1, 2, \ldots, m-2$ to give a new proof of Proposition 11.2.

11.6 (Conrad [Con]) Let $1 \le a_1, \ldots, a_r < q-1$ be integers; generalize the congruence (11.12) to

$$J(\omega_1^{a_1}, \ldots, \omega_r^{a_r}) \equiv \frac{(a_1 + \ldots + a_r)!}{a_1! \cdots a_r!} \bmod \mathcal{P}$$

for any $r \ge 2$. Here $J(\chi_1, \ldots, \chi_r)$ is the generalized Jacobi sum defined by

$$J(\chi_1, \ldots, \chi_r) = \sum_{\substack{t_1, \ldots, t_r \in \mathbb{F}_q \\ t_1 + \cdots + t_r = 1}} \chi_1(t_1) \cdots \chi_r(t_r).$$

11.7 Here we sketch the proof of Stickelberger's Relation as given in Davenport & Hasse [DaH]. Define a function $S(a)$ by $\mathcal{P}^{S(a)} \parallel G(\omega^a)$; we have to show that $S(a) = s(a)$.

$$S(\alpha) \ge 0 \tag{11.24}$$
$$S(\alpha + \beta) \le S(\alpha) + S(\beta) \tag{11.25}$$
$$S(\alpha + \beta) \equiv S(\alpha) + S(\beta) \bmod p - 1 \tag{11.26}$$
$$S(1) = 1 \tag{11.27}$$
$$S(\alpha p) = S(\alpha) \tag{11.28}$$
$$\sum_{\alpha \bmod q-1} S(\alpha) = \frac{f(p-1)(q-1)}{2} \tag{11.29}$$

Once we have proved these claims we can complete the proof as follows: from (11.24), (11.26) and (11.27) we deduce that $S(\alpha) \ge \alpha$ for $0 \le \alpha \le p-1$. From (11.25) and (11.27) we get $S(\alpha) \le \alpha$, and we conclude that $S(\alpha) = \alpha$ for $0 \le \alpha \le p-1$. Now (11.25) and (11.28) imply $S(\alpha) \le \alpha_0 + \ldots + \alpha_{f-1} = s(\alpha)$, where $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{f-1} p^{f-1}$. But now (11.29) gives

$$\sum_{\alpha \bmod q-1} S(\alpha) = \frac{1}{2} f(p-1)(q-2) = \sum_{\alpha \bmod q-1} s(\alpha),$$

and this implies the claim $S(\alpha) = s(\alpha)$. Now

- (11.24) follows directly from the fact that the Gauss sum $G(\chi)$ is an algebraic integer;
- (11.25) is also a direct consequence of the integrality of the Jacobi sums $J(\chi, \psi)$;
- (11.26) can be deduced from $J(\chi, \psi) \in \mathbb{Z}[\zeta_{q-1}]$;
- (11.27): redo the calculation we did in our proof of (11.2);
- (11.28): follows from $G(\omega^{ap}) = G(\omega^a)$;
- (11.29): note that $G(\omega^a)\overline{G(\omega^a)} = q$ implies $S(\alpha) + S(q-1-\alpha) = (p-1)f$ and form the sum over all $1 \le \alpha \le q-2$.

11.8 Prove Proposition 11.16 directly, that is, without using Stickelberger's Theorem 11.14.
Hints: 1. Show that it is sufficient to show that $\mathfrak{p}^h$ is principal for all prime ideals that split in k by using the fact that every ideal class contains an ideal prime to any given ideal (the only problem is to get around the ramified primes; an alternative solution is to show that ramified primes are principal if d is a prime discriminant, and that h is even otherwise).
2. Put $L = \mathbb{Q}(\zeta_m)$, where $m = |d|$, and observe that k is contained in the decomposition field K of p. Let $\mathfrak{P}$ denote a prime ideal above $\mathfrak{p}$ in $\mathcal{O}_K$; the following Hasse diagram (where $\widetilde{F} = F(\zeta_p)$) shows what's going on:

$$\begin{tikzcd}
\widetilde{L} \arrow[d, dash] \arrow[dr, dash] & & \\
\widetilde{K} \arrow[d, dash] \arrow[dr, dash] & L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\
\widetilde{k} \arrow[d, dash] \arrow[dr, dash] & K \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\
\mathbb{Q}(\zeta_p) \arrow[dr, dash] & k \arrow[d, dash] & \mathfrak{p} \arrow[d, dash] \\
 & \mathbb{Q} & (p)
\end{tikzcd}$$

Let $\chi = (\,\cdot\,/\mathfrak{P})_m^{-1}$ be the inverse of the m-th power character in $(\mathcal{O}_L/\mathfrak{P})^\times$, and let $G(\chi)$ denote the corresponding Gauss sum. Then $\mu = G(\chi)^m \in \mathcal{O}_K$ by Proposition 4.25. Show that $\mathfrak{p}^{(R-N)/m}$ is principal in $\widetilde{k}$.
3. Put $\gamma = N_{\widetilde{K}/\widetilde{k}} G(\chi)$; use an argument about ramification to show that $k(\gamma) = k$.

11.9 Use Stickelberger's congruence to prove the Davenport-Hasse theorem 4.32 (compare Exercise 10.28).
Hints: consider the algebraic number $\eta = G(\chi')/G(\chi)^{(E:F)}$.

1. Show that $\eta \in \mathbb{Q}(\zeta_m)$, where m denotes the order of χ (which equals the order of χ');
2. show that the prime ideal factorization of η contains only prime ideals above p;
3. show that η is a unit in $\mathbb{Z}[\zeta_m]$ (use the prime ideal factorization of the Gauss sum);
4. show that $|\eta| = 1$ and deduce that η must be a root of unity;
5. use Stickelberger's congruence to show that $\eta \equiv 1 \bmod \mathfrak{p}$ for any prime ideal $\mathfrak{p}$ above p in $\mathbb{Z}[\zeta_m]$ and conclude that $\eta = 1$.

Use the same idea to give a proof of the Davenport-Hasse relation in Theorem 4.31.

11.10 Let k be a totally real number field and K a totally complex quadratic extension. Show that $Q = (E_K : W_K E_k)$ divides 2.

11.11 Let M be a finite additive group on which a group $H = \{1, J\}$ of order 2 acts. Put $M^- = \{m \in M : Jm = -m\}$ and show that $(1-J)M \subseteq M^- \subseteq M$.Using $(1-J)M^- = 2M^-$, deduce that $2M^- \subseteq (1-J)M$.

11.12 Let $B \subseteq A$ be abelian groups and $f : A \longrightarrow A$ a group homorphism. Then $(A : B) = (A^f : B^f)(A_f + B : B)$ whenever these indices exist, where $A^f =$

$f(A)$, $B^f = f(B)$, and $A_f = \ker f$. Hint: show that the epimorphism $A/B \longrightarrow A^f/B^f$ has kernel $(A_f + B)/B$.

11.13 Let V be a $\mathbb{Q}$-vector space. An abelian group $A \subseteq V$ is called a lattice in V if $A = v_1\mathbb{Z} \oplus \ldots \oplus v_n\mathbb{Z}$, where $\{v_1, \ldots, v_n\}$ is a basis of V/F. Show that, given lattices A and B in V, there exists a lattice C in V containing A and B (can you find a counter example for vector spaces V over, say, $\mathbb{Q}(\sqrt{2}\,)$?). For any such lattice, define

$$(A : B) = \frac{(C : A)}{(C : B)},$$

where the indices on the right hand side are the usual indices of abelian groups, and show that this definition does not depend on the choice of C. Show that this index has the following properties:

i) $(A : B)$ coincides with the usual index if $B \subseteq A$;
ii) $(A : B) = (B : A)^{-1}$;
iii) $(A : B)(B : C) = (A : C)$.

11.14 (continued) Let A be a lattice in V, and assume that $T : V \longrightarrow V$ is a linear map with the property that there is an integer $m \in \mathbb{N}$ such that $mTA \subseteq A$. Then $(A : TA) = |\det T|$. Hints: $(A : TA) = (A : mTA)(mTA : TA) = (A : mTA)(TA : mTA)^{-1}$; clearly $(TA : mTA) = m^n$, so it is sufficient to show that $(A : TA) = |\det T|$ for any linear map $T : V \longrightarrow V$ such that $TA \subseteq A$. For help, cf. Cohn [Coh, IV.8, Lemma 7]. Alternatively, consider lattices $B \subseteq A$ and define $\operatorname{vol}(A)$ to be the volume of the parallelepiped spanned by the basis vectors of A. Show that $(A : B) = \operatorname{vol}(B)/\operatorname{vol}(A)$, and deduce our claim from $\operatorname{vol}(TA) = |\det T| \cdot \operatorname{vol}(A)$.

11.15 Verify the following table containing information about the subgroups of R occurring for $m = 3$ and $m = 4$ in our computation of the index of the Stickelberger ideal:

m	θ	$\mathcal{S}$	$\mathcal{S}^-$	$2e^-\mathcal{S}$	$I = \mathcal{S}\theta$	I^-
3	$\frac{1}{3}(1+2J)$	$(1+J,3)$	$3R^-$	$3R^-$	R	R^-
4	$\frac{1}{4}(1+3J)$	$(1+J,2-2J)$	$2R^-$	$4R^-$	$(1+J,1-J)$	R^-

Note that $I^- = (1-J)I$ for $m = 3$ while $(1-J)I = 2I^-$ for $m = 4$. Can you generalize?

11.16 Recall our proof that $2h^-$ kills the minus class group $\operatorname{Cl}(K^-)$ of $K = \mathbb{Q}(\zeta_p)$ and show that we have proved more, namely that twice the exponent of R^-/I^- annihilates $\operatorname{Cl}(K^-)$.

11.17 Let $\mathfrak{P}$ be a prime ideal in $K = \mathbb{Q}(\zeta_m)$ and put $\chi = (\,\cdot\,/\mathfrak{P})_m$. Show that $G(\chi)^m\mathcal{O}_K = \mathfrak{P}^{m\theta'}$, where $\theta' = m\sum_{(a,m)=1}\big(1 - \langle\frac{a}{m}\rangle\big)\sigma_a^{-1}$. Show that this implies $G(\chi)^m\mathcal{O}_K = \mathfrak{P}^{m(\nu/2+\theta_S)}$, where θ_S is the Brumer-Stark element for $K/\mathbb{Q}$ as defined in (11.17).

11.18 Verify the Brumer-Stark conjecture for cyclotomic extensions of $\mathbb{Q}$. Also show that $\theta_S = 0$ for real abelian extensions $K/\mathbb{Q}$.

11.19 Check what goes wrong in the proof of Proposition 11.16 if $d = -8$.

11.20 In the proof of Proposition 11.16, can you show that $\gamma \in k$ by Galois theory?

11.21 Prove Proposition 11.16 for ramified prime ideals. (Hint: if d is a prime discriminant, the claim is trivial since $\mathfrak{p}$ is principal in this case. If d is composite, $\mathfrak{p}^2 = (p)$ is principal, and it is sufficient to show that h is even).

11.22 (Washington [Was1, §6.2]) Let $K = \mathbb{Q}(\zeta_{12})$. Show that $\theta(K) = 1 + \sigma \in I(K) \setminus I_0(K)$.

11.23 Show that the integer defined in (11.15) gives $h^- = (N - R)/|d|$ for complex quadratic number fields of conductor d, and $h^- = \frac{1}{2}[(D_0 - D_2)^2 + (D_1 - D_3)^2]$ for complex cyclic quartic fields, where N, R and the D_j are defined in Propositions 11.16 and 11.18.

11.24 Show that the integer h^- defined in Proposition 11.18 is odd when the conductor f is an odd prime. Show that $h^- = 1$ for $f = 16$, and verify this by showing that the class number of $\mathbb{Q}(\sqrt{-2+\sqrt{2}}\,)$ is 1.

11.25 Let K/k be an extension of number fields. Define a map $j : \mathrm{Cl}\,(k) \longrightarrow \mathrm{Cl}\,(K)$ by mapping an ideal class $c = [\mathfrak{a}]$ to $[\mathfrak{a}\mathcal{O}_K] \in \mathrm{Cl}\,(K)$ and show that $\ker j$ is killed by $(K : k)$ (Hint: take the relative norm). Show that $\mathrm{Cl}^-(k)$ gets mapped to $\mathrm{Cl}^-(K)$.

11.26 For primes p, define a function $\Gamma_p : \mathbb{N} \longrightarrow \mathbb{Z}$ by $\Gamma_p(n) := (-1)^n \prod j$, where the product is over all $1 \le j \le n-1$ such that $p \nmid j$. Prove that $\Gamma_p(m+n) \equiv \Gamma_p(m) \bmod p^{v_p(n)}$ unless $p = 2$ and $n \equiv 4 \bmod 8$. Show that this congruence allows us to extend the function Γ_p continuously to a function $\Gamma_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times$ by putting $\Gamma_p(x) = \lim_{n \to x} \Gamma_p(n)$, where the n tend p-adically to $x \in \mathbb{Z}_p$. Verify that this p-adic Gamma function satisfies $\Gamma_p(0) = 1$, and that $\Gamma_p(x+1)/\Gamma_p(x) = -x$ or $= -1$ according as $x \in \mathbb{Z}_p^\times$ or $x \in p\mathbb{Z}_p$.

11.27 A non-empty set I is called *partially ordered* if there is an order relation $<$ defined on I such that

1. $i < j$ and $j < k \Longrightarrow i < k$;
2. $i < j$ and $j < i \Longrightarrow i = j$;
3. $i < i$ for all $i \in I$.

The set I is called *directed* if, in addition, it has the property

1. for all $i, j \in I$ there is a $k \in I$ such that $i < k$ and $j < k$.

Now consider a family X_i $(i \in I)$ of compact topological spaces indexed by a directed set I, and assume that for each pair $(i,j) \in I \times I$ there exists a continuous epimorphism $\pi_{ij} : X_j \longrightarrow X_i$ such that
i) $\pi_{ii} = \mathrm{id}$;
ii) if $i < j < k$, then $\pi_{ij} \circ \pi_{jk} = \pi_{ik}$;
then the triple $(X_i; \pi_{ij}; I)$ is called an *projective system.*

Given such a projective system, we can form the direct product $\widetilde{X} = \prod_{i \in I} X_i$ and make it into a topological space by giving it the product topology; this ensures that the projection maps $\pi_i : \widetilde{X} \longrightarrow X_i$ are continuous. Now define the *projective limit* of this projective system by

$$\varprojlim X_i = \{x \in \widetilde{X} : \pi_{ij} \circ \pi_j(x) = \pi_i(x) \text{ for all } i < j\}.$$

1. Use the axiom of choice to show that $\varprojlim X_i$ is non-empty;
2. Use Tychonov's theorem to show that $\varprojlim X_i$ is compact;
3. Show that X is a group if each X_i is a group;
4. For a ring R, show that X is an R-module if each X_i is.

11.28 Let ℓ be a prime and consider the finite groups $X_n = \mathbb{Z}/\ell^n\mathbb{Z}$ together with the projections $\pi_{mn} : \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow \mathbb{Z}/\ell^m\mathbb{Z}$ for $0 < m < n$. Endow the X_n with the discrete topology and show that the triple $(X_n; \pi_{mn}; \mathbb{N})$ is a projective system. Show that $\varprojlim X_n \simeq \mathbb{Z}_\ell$ as topological groups, where the topology on $\mathbb{Z}_\ell$ is induced by the ℓ-adic valuation.

11.29 Let $K_0 \subseteq K_1 \subseteq \ldots$ be a tower of normal number fields, and put $G_n = \mathrm{Gal}\,(K_n/K_0)$. Define epimorphisms $\pi_{mn} : G_n \longrightarrow G_m$ for $m < n$ such that $(G_n; \pi_{mn}; \mathbb{N})$ becomes a projective system, and show that $\mathcal{G} = \varprojlim G_n$ is topologically isomorphic to the Galois group of $K_\infty = \bigcup_n K_n$, endowed with the Krull topology.

11.30 Let $K = K_0 \subset K_1 \subset \ldots \subset K_n \subset \ldots$ be a $\mathbb{Z}_p$-extension of a number field K, that is, a family of number fields such that $\mathrm{Gal}\,(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ (the preceding exercise shows that $\mathrm{Gal}\,(K_\infty/K) \simeq \mathbb{Z}_p$). Put $A_n = \mathrm{Cl}_p(K_n)$ and show that the relative norms $N_{mn} = N_{K_n/K_m}$ make $(A_n; N_{mn}; \mathbb{N})$ into a projective system.

11.31 Put $K = \mathbb{Q}(\sqrt{-5}\,)$ and $L = K(i)$. Show that the result of Hilbert and Speiser is not valid for general number fields by showing that L/K is unramified (hence tame), that $\mathcal{O}_L$ has an integral basis over $\mathcal{O}_K$, but does not have a NIB over $\mathcal{O}_K$.

11.32 (Furtwängler 1912) Let p be an odd prime, and assume that $x^p + y^p + z^p = 0$ for pairwise coprime integers $x, y, z \in \mathbb{Z}$ with $p \nmid xyz$. Use the unique factorization theorem for prime ideals to deduce that $(x + y\zeta^i) = \mathfrak{A}_i^p$ for ideals $\mathfrak{A}_i$, $i = 0, 1, \ldots, p-1$. Show that $\alpha = \zeta^y x + \zeta^{-x} y$ is semi-primary. Now use Eisenstein's reciprocity law to deduce that $\left(\frac{\alpha}{r}\right)_p = \left(\frac{r}{\alpha}\right)_p = \left(\frac{r}{\mathfrak{A}_j}\right)_p^p = 1$ for each prime $r \mid x$, and deduce that $r^{p-1} \equiv 1 \bmod p^2$.

11.33 (Wieferich 1909) Suppose that $x^p + y^p + z^p = 0$ for some odd prime $p \nmid xyz$; then $2^{p-1} \equiv 1 \bmod p^2$. (Hint: Use the preceding exercise).
Remark. Primes p satisfying $2^{p-1} \equiv 1 \bmod p^2$ are called *Wieferich primes*. The only Wieferich primes below $4 \cdot 10^{12}$ are 1093 and 3511 (see Crandall, Dilcher & Pomerance [CDP]).

11.34 (S. Germain 1823) Suppose that $x^p + y^p + z^p = 0$ for some odd prime $p \nmid xyz$; then $\ell = 2p + 1$ is not prime.

11.35 (Legendre 1823) Suppose that $x^p + y^p + z^p = 0$ for some odd prime $p \nmid xyz$; then the numbers $2p + 1, 4p + 1$ and $8p + 1$ are not prime.

11.36 (Furtwängler 1912) Suppose that $x^p + y^p + z^p = 0$ for some odd prime $p \nmid xyz$, and that $(x, y) = (y, z) = (x, z) = 1$; assume moreover that $p \nmid (x^2 - y^2)$; then $r^{p-1} \equiv 1 \bmod p^2$ for every prime $r \mid (x - y)$.

11.37 (Mirimanoff 1911) Suppose that $x^p + y^p + z^p = 0$ for some prime $p \nmid xyz$, $p > 3$; then $3^{p-1} \equiv 1 \bmod p^2$.

11.38 Transform the Fermat curve $x^3 + y^3 = 1$ into Weierstraß form. (Hint: put $x = u + v$, $y = u - v$).

11.39 Transform the Fermat curve $w^4 + 1 = z^2$ into Weierstraß form. (Hint: write it as $1 = (w^2 - z)(w^2 + z)$ and put $x = w^2 + z$. Then $2w^2 = x + \frac{1}{x}$; multiply by x^2 and put $wx = y$).

11.40 Ribenboim [Ri1] sketches a proof for FLT in the case $n = 7$; fill in the details and transform the resulting curve $u^2 = s^4 + 6s^2t^2 - \frac{1}{7}t^4$ into the form $E : y^2 = x(x^2 - 3\cdot 7^2 x + 16\cdot 7^3)$. Use simple 2-descent to show that $E(\mathbb{Q}) = E(\mathbb{Q})_{\rm tors} \simeq \mathbb{Z}/2\mathbb{Z}$, and conclude that $x^7 + y^7 = z^7$ has only trivial solutions in $\mathbb{Z}$.

Additional References

[An] G.W. Anderson, *Another look at the index formulas of cyclotomic number theory*, J. Number Theory **60** (1996), 142–164

[Ba] P. Bachmann, *Das Fermatproblem in seiner bisherigen Entwicklung*, Reprint Springer-Verlag 1976

[Bau] H. Bauer, *Zur Berechnung von Hilbertschen Klassenkörpern mit Hilfe von Stark-Einheiten*, Diss. TU Berlin, 1998

[BC] M. Bertolini, G. Canuto, *The Shimura-Taniyama-Weil conjecture* (Italian), Boll. Unione Mat. Ital. (VII) **10** (1996), 213-247

[Br1] J. Brinkhuis, *Gauss sums and their prime factorization*, Ens. Math. **36** (1990), 39–51

[Br2] J. Brinkhuis, *On a comparison of Gauss sums with products of Lagrange resolvents*, Compos. Math. **93** (1994), 155–170

[Br3] J. Brinkhuis, *Normal integral bases and the Spiegelungssatz of Scholz*, Acta Arith. **69** (1995), 1–9

[BC1] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. **61** (1993), 151–153

[BC2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M.A. Shokrollahi, *Irregular primes and cyclotomic invariants to eight million*, J. Symbolic Computation **11** (1998)

[CT] Ph. Cassou-Noguès, M.J. Taylor, *Un élément de Stickelberger quadratique*, J. Number Theory **37** (1991), 307–342

[Cau] A.L. Cauchy, *Mémoire sur la théorie des nombres; Note VIII*, Mém. Inst. France **17** (1840), 525–588 Œuvres (1) III, 265–292

[Ch1] R.J. Chapman, *A simple proof of Noether's theorem*, Glasg. Math. J. **38** (1996), 49–51

[Ch2] R.J. Chapman, `http://www.maths.ex.ac.uk/~rjc/rjc.html`

[Cho] S. Chowla, *L-series and elliptic curves*, Lecture Notes Math. **626**, Springer 1977, 1–42

[Co1] J. Coates, *On K_2 and some classical conjectures in algebraic number theory*, Ann. of Math. **95** (1972), 99–116

[Co2] J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields, Durham 1975, (1977), 269–353

[Co3] J. Coates, *The work of Mazur and Wiles on cyclotomic fields*, Semin. Bourbaki 1980/81, Exp. 12, Lect. Notes Math. **901** (1981), 220–241

[CGR] J. Coates, R. Greenberg, K. Ribet, K. Rubin, C. Viola, *Arithmetic Theory of Elliptic Curves*, CIME Lectures 1997, Springer LNM 1716, 1999

[CoP] J. Coates, G. Poitou, *Du nouveau sur les racines de l'unité*, Gaz. Math., Soc. Math. Fr. **15** (1980), 5–26

[CoS] J. Coates, W. Sinnott, *An analogue of Stickelberger's theorem for the higher K-groups*, Invent. Math. **24** (1974), 149–161

[Coh] H. Cohn, *Advanced Number Theory*, Dover 1980

[Con] K. Conrad, *Jacobi sums and Stickelberger's congruence*, L'Enseign. Math. **41** (1995), 141–153

[CSS] G. Cornell, J.H. Silverman, G. Stevens (eds.), *Modular Forms and Fermat's Last Theorem*, Springer 1997

[Cox] D.A. Cox, *Introduction to Fermat's Last Theorem*, Amer. Math. Mon. **101** (1994), 3–14

[CDP] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449

[Dar] H. Darmon, *The Shimura-Taniyama conjecture (d'apres Wiles)*, Russ. Math. Surv. **50** (1995), 503–548; translation from Usp. Mat. Nauk **50** (1995), 33–82

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*, Current developments in mathematics, Cambridge International Press (1995), 1–107

[DaH] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182

[DeR] P. Deligne, K.A. Ribet, *Values of Abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), 227–286

[DuH] D.S. Dummit, D.R. Hayes, *Checking the $\mathfrak{p}$-adic Stark Conjecture*, ANTS II, Lecture Notes Comput. Sci. **1122** (1996), 91–97

[DST] D.S. Dummit, J.W. Sands, B.A. Tangedal, *Computing Stark units for totally real cubic fields* Math. Comput. **66** (1997), 1239–1267

[Eis] G. Eisenstein, *Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ und $7n+4$*, J. Reine Angew. Math. **37** (1848), 97–126; Werke II, 506–535

[Ere] B. Erez, *Representations of groups in algebraic number theory. An introduction* (Ital.), Proc. Colloq., Locarno/Italy 1988-1989, Note Mat. Fis. (3) (1990), 41–65

[Er1] R. Ernvall, *Generalized Bernoulli numbers, generalized irregular primes, and class number*, Ann. Univ. Turku **178** (1979), 72 pp.

[Er2] R. Ernvall, *A generalization of Herbrand's theorem*, Ann. Univ. Turku, Ser. A I **193** (1989), 15 pp.

[EM] R. Ernvall, T. Metsänkylä, *Cyclotomic invariants and E-irregular primes* Math. Comp. **32** (1978), 617–629; Corr.: ibid. **33** (1979), 433

[Fe] L.J. Federer, *Regulators, Iwasawa modules, and the main conjecture for $p = 2$*, Number theory related to Fermat's last theorem, Prog. Math. **26** (1982), 287–296

[FG] G.J. Fee, A. Granville, *The prime factors of Wendt's Binomial Circulant determinant*, Math. Comp. **57** (1991), 839–848

[Fro] G. Frobenius, *Über den Fermat'schen Satz III*, Sitzungsber. Akad. Wiss. Berlin (1914), 653–681

[Fr1] A. Fröhlich, *Galois module structure of algebraic integers*, Springer-Verlag 1983

[Fr2] A. Fröhlich, *Stickelberger without Gauss sums*, Algebraic Number fields, Univ. Durham 1975, 589–607 (1977)

[FQ] A. Fröhlich, J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. **20** (1973), 125–138

[Gha] E. Ghate, *Vandiver's conjectue via K-theory*, Summer School on Cyclotomic Fields, June 1999; preprint, see
`http://www.math.tifr.res.in/~eghate/`

[Gil] R. Gillard, *Relations de Stickelberger*, Sém. Théor. Nombres Grenoble, 1974

[Gr1] A. Granville, *Sophie Germain's Theorem for prime pairs p, $6p+1$*, J. Number Theory **27** (1987), 63–72

[Gr2] A. Granville, *The Kummer-Wieferich-Skula approach to the First Case of Fermat's Last Theorem*, Advances in Number Theory (F.Q. Gouvea, N. Yui, eds.), Oxford University Press 1993, 479–498

[GM] A. Granville, M.B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* $714,591,416,091,389$, Trans. Am. Math. Soc. **306** (1988), 329–359

[Gra] G. Gras, *Sommes de Gauss sur les corps finis*, Publ. Math. Besançon (1977/78), 71 pp

[Gre] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier **42** (1991), 449–500

[GRR] C. Greither, D.R. Replogle, K. Rubin, A. Srivastav, *Swan modules and Hilbert-Speiser number fields*, preprint 1999

[GK] B.H. Gross, N. Koblitz, *Gauss sums and the p-adic Γ-function*, Annals of Math. **109** (1979), 569–581

[Gut] M. Gut, *Euler'sche Zahlen und Klassenzahl des Körpers der 4ℓ-ten Einheitswurzeln*, Commentarii Math. Helvet. **25** (1951), 43–63

[HP] G. Harder, R. Pink, *Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbb{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen*, Math. Nachr. **159** (1992), 83–99

[Has1] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag Berlin 1952; Reprint Akademie-Verlag Berlin 1985

[Has2] H. Hasse, *Letter to Davenport, May 20, 1934*, Trinity College, Cambridge, UK.

[Hay1] D.R. Hayes, *Hecke characters and Eisenstein reciprocity in function fields*, J. Number Theory **43** (1993), 251–292

[Hay2] D.R. Hayes, *The conductors of Eisenstein characters in cyclotomic number fields*, Finite Fields Appl. **1** (1995), 278–296

[Hec] E. Hecke, *Über nicht-reguläre Primzahlen und den Fermatschen Satz*, Gött. Nachr. (1910), 420–424

[Hll] Y. Hellegouarch, *Invitation aux mathematiques de Fermat-Wiles*, Paris: Masson, 397 pp, 1997

[Hel] C. Helou, *On Wendt's determinant*, Math. Comput. **66** (1997), 1341–1346

[Her] J. Herbrand, *Sur les classes des corps circulaires*, J. Math. Pures Appl. **11** (1932), 417–441

[Hrt] C. Hermite, *Lettre à Jacobi, Aug. 06, 1845*, Œuvres de Charles Hermite I, 100–121

[Ibr] I. Ibrahimoglu, *A proof of Stickelberger's theorem*, Hacettepe Bull. Nat. Sci. Eng. **12** (1983), 279–287

[Jac] C. G. J. Jacobi, *Observatio arithmetica de numero classium divisorum quadraticorum formae $yy+Azz$, designante A numerum primum formae* $4n+3$, J. Reine Angew. Math. **9** (1832), 189–192; Ges. Werke **6**, 240–244, Berlin 1891

[Jha] V. Jha, *The Stickelberger ideal in the spirit of Kummer with application to the first case of Fermat's last theorem*, Queen's Papers in Pure and Applied Mathematics **93**, 181 pp. (1993)

[Joh] W. Johnson, *p-adic proofs of congruences for the Bernoulli numbers*, J. Number Theory **7** (1975), 251–265

[Ka] S. Kamienny, *Modular curves and unramified extensions of number fields*, Compositio Math. **47** (1982), 223–235

[KM] I. Kersten, J. Michalicek, *On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\zeta_{p^n})$*, J. Number Theory **32** (1989), 371–386

[Kim] T. Kimura, Algebraic class number formulae for cyclotomic fields (Japanese), Sophia University, Department of Mathematics. IX, 281 pp. (1985)

[Kle] H. Kleboth, *Untersuchung über Klassenzahl und Reziprozitätsgesetz im Körper der 6ℓ-ten Einheitswurzeln und die Diophantische Gleichung $x^{2\ell}+31y^{2\ell}=z^{2\ell}$ für eine Primzahl ℓ grösser als* 3, Diss. Univ. Zürich 1955, 37 pp.

[Klj] T. Kleinjung, *Konstruktion unverzweigter Erweiterungen von Zahlkörpern durch Wurzelziehen aus zyklotomischen Einheiten*, Diplomarbeit Univ. Bonn, 1994

[Kob] N. Koblitz, *p-adic analysis: a short course on recent work*, London Math. Soc. LNS **46**, 1980

[Kol] M. Kolster, *A relation between the* 2*-primary parts of the main conjecture and the Birch-Tate-conjecture*, Can. Math. Bull. **32** (1989), 248–251

[Kr1] J. Kramer, *Über die Fermat-Vermutung*, Elem. Math. **50** (1995), 12–25

[Kr2] J. Kramer, *Über den Beweis der Fermat-Vermutung. II*, Elem. Math. **53** (1998), 45–60

[Kub] T. Kubota, *An application of the power residue theory to some abelian functions*, Nagoya Math. J. **27** (1966), 51–54

[Kur] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compos. Math. **81** (1992), 223–236

[La1] S. Lang, *Algebraic Number Theory*, Addison-Wesley 1970; reissued as Graduate Texts in Mathematics **110**, Springer-Verlag 1986; 2nd. ed. 1994

[La2] S. Lang, *Cyclotomic fields. I and II*, Graduate Texts in Mathematics **121**, Springer-Verlag 1990

[La3] S. Lang, *Classes d'idéaux et classes de diviseurs*, Semin. Delange-Pisot-Poitou 1976/77, Exp. 28, 9 pp. (1977)

[Lan] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927; Chelsea 1969

[Leg] A. M. Legendre, , Mem. Acad. Sci. Inst. France **6** (1823), 1–60; see also Théorie des nombres, 2nd ed. (1808), second supplement (1825), 1–40.

[LeSt] H. W. Lenstra, P. Stevenhagen, *Class field theory and the first case of Fermat's Last Theorem*, see [CSS], 499–503 (1997).

[Leo] H. W. Leopoldt, *Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174

[Lip] M. Lippert, *Konstruktion unverzweigter Erweiterungen von Zahlkörpern durch Wurzelziehen aus Elementen eines Eulersystems*, Diplomarbeit Univ. Bonn, 1996

[McK] R.E. MacKenzie, *Class group relations in cyclotomic fields*, Amer. J. Math. **74** (1952), 759–763

[Ma1] J. Martinet, *Bases normales et constante de l'équation fonctionelle des fonctions L d'Artin*, Sém. Bourbaki 1973/74, Exposé 450, Lecture Notes Math. **431** (1975), 273–294

[Ma2] J. Martinet, H_8, Algebr. Number Fields, Proc. Symp. London Math. Soc., Univ. Durham 1975, 525–538 (1977)

[MW] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179–330

[Met] T. Metsänkylä, *The index of irregularity of primes*, Expo. Math. **5** (1987), 143–156

[Mir1] M. D. Mirimanoff, *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris **150** (1910), 204–206

[Mir2] M. D. Mirimanoff, *Sur le dernier théorème de Fermat*, J. Reine Angew. Math. **139** (1911), 309–324

[Mi1] H.H. Mitchell, *On the generalized Jacobi-Kummer cyclotomic function*, Amer. Math. Soc. Trans. **17** (1916), 165–177; FdM **46** (1916–18), 255

[Mi2] H.H. Mitchell, *Proof that certain ideals in a cyclotomic realm are principal ideals*, Trans. Amer. Math. Soc. **19** (1918), 119–126

[Mo1] C.J. Moreno, *Algebraic curves over finite fields*, Cambridge Tracts in Mathematics **97**, CUP 1991

[Mo2] C.J. Moreno, *Fermat's Last Theorem: From Fermat to Wiles*, Rev. Colomb. Mat. **29** (1995), 49–88

[Mu1] V.K. Murty, *Fermat's last theorem*, Analysis, geometry and probability, Texts Read. Math. **10** (1996), 125–139

[Mu2] V.K. Murty, *Modular elliptic curves*, Seminar on Fermat's last theorem, CMS Conf. Proc. **17** (1995), 1–38

[Mu] M.R. Murty, *Topics in Number Theory*, Lecture Notes 1993

[Nar] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Warszawa 1974; 2nd ed. Springer-Verlag 1990

[Nek] J. Nekovar, *Iwasawa's main conjecture. (A survey)*, Acta Math. Univ. Comenianae **50/51** (1987), 203–215

[Noe] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152

[Nog] R. Nogues, *Théorème de Fermat: son histoire*, Paris 1932; 2nd ed. 1966; reprint of 1st ed. Sceaux 1992

[Ou] Yi Ouyang, *Spectral sequence of universal distribution and Sinnott's index formula*, preprint 1999;
`http://front.math.ucdavis.edu/math.NT/9911031`

[PR] B. Perrin-Riou, *Travaux de Kolyvagin et Rubin*, Semin. Bourbaki, Vol. 1989/90, Astérisque **189-190**, Exp. No. 717 (1990), 69–106

[Pol] F. Pollaczek, *Über die irregulären Kreiskörper der ℓ-ten und ℓ^2-ten Einheitswurzeln*, Math. Z. **21** (1924), 1–37

[Ras] R. Rashed, *The development of Arabic mathematics: between arithmetic and algebra*, Kluwer 1994

[Ri1] P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag 1979

[Ri2] P. Ribenboim, *Fermat's Last Theorem, before June 23, 1993*, Number theory (K. Dilcher, ed.), Mathematical Society, CMS Conf. Proc. **15** (1995), 279–294

[Rb1] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162

[Rb2] K. Ribet, *Galois representations and modular forms*, Bull. Am. Math. Soc. **32** (1995), 375–402

[Rid] D. Rideout, *A generalization of Stickelberger's theorem*, thesis, McGill University, Montreal 1970

[Ro1] X.-F. Roblot, *Unités de Stark et corps de classes de Hilbert*, C. R. Acad. Sci., Paris **323** (1996), 1165–1168

[Ro2] X.-F. Roblot, *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon*, Diss. Univ. Bordeaux, 1997

[Ru1] K. Rubin, *Kolyvagin's system of Gauss sums*, Arithmetic algebraic geometry, Prog. Math. **89** (1991), 309–324

[Ru2] K. Rubin, *Euler systems and exact formulas in number theory*, Jahresber. DMV **98** (1996), 30–39

[Sal] H. Salié, *Eulersche Zahlen*, Sammelband Leonhard Euler, Deutsche Akad. Wiss. Berlin 293–310 (1959)

[San] J.W. Sands, *Abelian fields and the Brumer-Stark conjecture*, Compositio Math. **53** (1984), 337–346

[Sf1] R. Schoof, *Fermat's Last Theorem*, Jahrbuch Überblicke Math. 1995 (Beutelspacher, ed.), Vieweg 1995, 193–211

[Sf2] R. Schoof, *Wiles' proof of Taniyama-Weil conjecture for semi-stable elliptic curves over* $\mathbb{Q}$, Gaz. Math., Soc. Math. Fr. **66** (1995), 7–24

[Sf3] R. Schoof, *Minus class groups of the fields of the* l*th roots of unity*, Math. Comp. **67** (1998), 1225–1245

[Sch] K. Schwering, *Zur Theorie der arithmetischen Funktionen, welche von Jacobi* $\psi(\alpha)$ *genannt werden*, J. Reine Angew. Math. **93** (1882), 334–337

[ST] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Tokyo 1961

[Shi] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo **23** (1976), 393–417

[Sin] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234

[Sol] D.R. Solomon, *On the class groups of imaginary abelian fields*, Ann. Inst. Fourier **40** (1990), 467–492

[Sou] C. Soulé, *Perfect forms and the Vandiver conjecture*, J. Reine Angew. Math. **517** (1999), 209–221

[Sp] A. Speiser, *Gruppendeterminante und Körperdiskriminante*, Math. Annalen **77** (1916), 546–562

[Su] J. Suzuki, *On the generalized Wieferich criteria*, Proc. Japan Acad. **70** (1994), 230–234

[Tak] T. Takagi, *Zur Theorie des Kreiskörpers*, J. Reine Angew. Math. **157** (1927), 230–238; Coll. Papers 246–255

[Ta] G. Tamme, *Über die* p*-Klassengruppe des* p*-ten Kreisteilungskörpers*, Ber. Math.-Stat. Sekt. Joanneum (1988), 48 pp.

[Ta1] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Math. (J. Coates, S. Helgason, eds), Birkhäuser, 1984

[Ta2] J. Tate, *Brumer-Stark-Stickelberger*, Sémin. Theor. Nombres 1980–1981, Exp. No. **24** (1981), 16 pp.

[Ter] G. Terjanian, *Sur l'équation $x^{2p} + y^{2p} = z^{2p}$*, C. R. Acad. Sci. Paris **285** (1977), 973–975

[Tha] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. Math. **128** (1988), 1–18

[vdP] A. van der Poorten, *Notes on Fermat's last theorem*, Wiley, New York 1996

[Vor] G.F. Voronoi, Über die Summe der quadratischen Reste einer Primzahl $p = 4m + 3$ (Russ.), St. Petersb. Math. Ges. **5**; FdM **30** (1899), 184

[Was1] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer Verlag 1982; 2nd edition 1997

[Was2] L. C. Washington, *Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine*, Number Theory (eds.: J.-M. de Koninck, C. Levesque), Proceedings of the Intern. Number Theory Conference at Laval (1987) W. Gruyter, Berlin, New York, 990–993

[WSS] T. Washio, A. Shimaura, K. Shiratani, *On certain congruences for Gauss sums*, Sci. Bull. Fac. Educ., Nagasaki Univ. **55** (1996), 1–8

[Wen] E. Wendt, *Arithmetische Studien über den "letzten" Fermatschen Satz, welcher aussagt, daß die Gleichung $a^n = b^n + c^n$ für $n \geq 2$ in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math. **113** (1894), 335–347

[Wie] A. Wieferich, *Zum letzten Fermatschen Theorem*, J. Reine Angew. Math. **136** (1909), 293–302

[Wil] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540

[WHS] K.S. Williams, K. Hardy, B.K. Spearman, *Explicit evaluation of certain Eisenstein sums*, Number theory, Banff/Alberta 1988, 553–626 (1990)