Errata and Additions to "Reciprocity Laws. From Euler to Eisenstein".

page	for	read
p. ix, line – 7	finite extension	finite normal extension
p. x, line –12	that to look	that one should look
p. xi, line –7	solutions $ax^4 - by^4 = 1$	solutions of $ax^4 - by^4 = 1$
p. xiii, line –5	presentation	presentation of
p. xiv, line 5	but it hope	but I hope
p. 15, line – 13	towards of	towards
p. 25, line 22	$p \equiv q \equiv 1 \bmod 4$	$p \equiv q \equiv 3 \bmod 4$
p. 28, Exer. 1.8.	$l_p = rx + sy = tz$	$l_p = rx + sy + tz$
p. 30, line 5	residcovered	rediscovered
p. 32, line – 5	$A, B, M, N \in \mathbb{N}$	$A, B, M, N \in \mathbb{Z}$
p. 43, line – 13	$X + (X^2 - m)\mathbb{Z}[X]$	$X + (X^2 - m)\mathbb{Q}[X]$
p. 44, lines 9–11	$m < -4$, $m = -4$	disc $k < -4$, disc $k = -4$
p. 47, Proof Prop. 2.8	$\lambda^{-1}\mathfrak{a} = \mathfrak{c}^{\sigma-1}$	$\lambda^{-1}\mathfrak{a} = \mathfrak{c}^{1-\sigma}$
p. 60, line – 14	p-adic square	2-adic square
p. 61, line –3	implies that	implies
p. 64, iii)	$\left(\frac{m,n}{p}\right)$	$\left(\frac{a,b}{p}\right)$
p. 66, Thm. 2.30	$\prod_{p\geq 2}$	$\bigoplus_{p\geq 2}$
p. 70, line – 11	reciprocity law)	reciprocity law
p. 71, line – 5	$(p/q) = +1$	$(p/q) = -1$
p. 73, line – 3	every factor	every odd factor
p. 74, Ex. 2.29.	ε_p	ε_q
p. 76, Ex. 2.29.	$p^h = 4a^2 + qb^2$	$p^h = 4a^2 + qb^2$
p. 83, Prop. 3.4	$\sqrt{p^*}\mathbb{Z}$	$\sqrt{p^*}\mathbb{Z}[X]$
p. 88, Cor. 3.10.vi)	$\mathfrak{P}$	$\mathfrak{p}$
p. 92, line – 11	possible improve	possible to improve
p. 92, Thm. 3.18	integers smallest	smallest
p. 99, lines 8, 11	$\left(\frac{2}{p}\right)\prod$	$\prod$

page	for	read
p. 101, line 6	g of p	g modulo p
p. 101, line 9	b	$a+1$
p. 102, footnote line 1	restricted us	restricted ourselves
p. 111, line – 13	an n-th root	a primitive n-th root
p. 112, 4.2.iii)	$\alpha \in \mathcal{O}_k$	$\alpha \in \mathcal{O}_K$
p. 112, line 7	$\xi \in \mathcal{O}_k$	$\xi \in \mathcal{O}_k \setminus \mathfrak{p}$
p. 113, line – 2	$(\frac{\alpha}{\mathfrak{p}})_k$	$(\frac{\alpha}{\mathfrak{p}})_K$
p. 113, line – 2	$(\frac{\alpha}{\mathfrak{P}})_k^{(K:k)}$	$(\frac{\alpha}{\mathfrak{P}})_K^{(K:k)}$
p. 126, line -3	π	Π
p. 130, Prop. 4.25	of $\mathfrak{p}$.	of $\mathfrak{p}$ in $\mathbb{Q}(\zeta_{mp})$.
p. 130, Prop. 4.25.ii)	$\mathbb{Q}(\zeta_m)$	$\mathbb{Q}(\zeta_{mp})$
p. 130, line 18	of the Artin	of the Artin symbol
p. 131, Prop. 4.28	$= fp$	$\mathfrak{p}$
p. 135, lines –13, –14	$\mathbb{F}\,\mathbb{1}$	$\mathcal{F}\,\mathbb{1}$
p. 136, line 10	[Wy1,Wy2,Why]	[Why] and [Wy1,Wy2] in Ch. 1
p. 158, line 9	desired equality (5.5)	desired equality (5.3)
p. 162, line – 2	$(\frac{p}{q})_4(\frac{\varepsilon}{p})$	$(\frac{p}{q})_4(\frac{\varepsilon}{q})$
p. 167, line – 9	$p \mid ABC$	$q \mid ABC$
p. 167, line – 6	$m = q$	$m = p$
p. 174, line – 10	of Chapter 6.7,9	of Chapters 6, 7 and 9
p. 181, 5.35	mod p.	mod p, where $p = c^2 + 5d^2$.
p. 189, line -1	$(\frac{\ell^*}{p})_4$	$\left(\frac{\ell^*}{p}\right)_4$
p. 190, table	11	-11
p. 236, line -5	$a_i \in \mathbb{Z}$	$a_i \in \mathbb{Z}[\frac{1}{2}]$
p. 246, line -8	$\phi\Big(\frac{\alpha}{\mu}\Big)$	$\phi\Big(\frac{\alpha}{\mu}\Big)$
p. 265, line 3	$K(j(\sqrt{-5})) = K(\sqrt{2})$	$K(j(\sqrt{-5})) = K(\sqrt{-1}\,)$
p. 280, Ex. 8.19	$[\kappa/\pi = [\pi^*/\kappa]$	$[\kappa/\pi] = [\pi^*/\kappa]$
p. 294, Prop. 9.5.	$c \equiv \frac{p-3}{4} \bmod 4$	$c \equiv -\frac{p+1}{4} \bmod 4$

page	for	read
p. 300, lines –8 to – 6	$\phi(\frac{*}{z})$	$\phi(\frac{*}{\pi})$
p. 302, line −14	did no repeat	did not repeat
p. 312, line 3	Theorem 9.18	Theorem 9.19
p. 315, Ex. 9.9.	computer.	computer).
p. 318, line 16	$x^2 + 1 \neq 0$	$v^2 + 1 \neq 0$
p. 319, line 3	$(\pm i, 0)$, $(0, \pm i)$	$(w, v) = (\pm i, 0)$, $(0, \pm i)$
p. 321, line – 15	m-the	m-th
p. 330, line 3	$2n \leq 50$	$2n \leq 32$
p. 351, Cartier	fonction zeta,	fonction zeta),
p. 355, line – 4	J.F. Felipe	J.F. Voloch
p. 372, line 12	elementattached	element attached
p. 372, line 15	$\sum \alpha < m/2\sigma_a^{-1}$	$\sum_{\alpha<m/2} \sigma_a^{-1}$
p. 376, lines −3, −1	ε_i	e_i
p. 377, line 2	ε_i	e_i
p. 377, lines 4, 8	e_χ	e_i
p. 378, lines 2, 4, 8	mC_i	$\mathcal{C}_i$
p. 380, line −12	$e_\chi\theta = B_{1,\chi^{-1}}\theta$	$\theta\varepsilon_\chi = B_{1,\chi^{-1}}\varepsilon_\chi$
p. 394, line –10	annihilate	annihilates
p. 406, Kleboth	Gle-ichung	Glei-chung
p. 415, Teege 2	1921	1925
p. 418, 7th problem	Eisenstein sums	elliptic Gauss sums
p. 422, [55]	Minkowsi–Hasse	Minkowski–Hasse
p. 444, [424]	Yamamoto	Yamamoto,
p. 462, [735]	Sierpinsky	Sierpinski
p. 467, [808]	1895/86	1895/96

Prop. 1.5.

This is of course nonsense. What I (probably) meant is that if $fx^2 + gy^2 = hz^2$ has integral solutions, then gh (hf, $-fg$) are quadratic residues modulo every prime divisor of f (g, h).

Lemma 3.13

The discussion involving the index m ended up in the wrong part of the proof. Here's the correction:

Assume that there exists a ring homomorphism $\psi : \mathcal{O} \longrightarrow \mathbb{Z}/n\mathbb{Z}$; since $\mathbb{Z}[\alpha] \subseteq \mathcal{O}$ is a subring, the composition of restriction and the isomorphism $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(f)$ gives a ring homomorphism $\widehat{\psi} : \mathbb{Z}[X]/(f) \longrightarrow \mathbb{Z}/n\mathbb{Z}$. Now let $a \in \mathbb{N}$ be an integer such that $a + n\mathbb{Z} = \widehat{\psi}(X + (f))$. Then $f(a) + n\mathbb{Z} = \widehat{\psi}(f(X) + (f)) = \widehat{\psi}(0) = 0 + n\mathbb{Z}$, and so $n \mid f(a)$ as claimed.

Conversely, given $a \in \mathbb{Z}$ with $n \mid f(a)$, we can define a ring homomorphism $\widehat{\psi} : \mathbb{Z}[X]/(f) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ by mapping $X + (f)$ to $a + n\mathbb{Z}$. This can be extended to a ring homomorphism $\mathcal{O} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ by putting $\psi(\beta) = m^{-1}\widehat{\psi}(m\beta)$ for any $\beta \in \mathcal{O}$: in fact, m is invertible modulo n by assumption, and $m\beta \in \mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}$.

Rational Reciprocity

Chapter 5, p. 165, line –1: for the last equivalence to be valid for primes $q \mid C$, we have to interpret the quadratic residue symbol as a Kronecker symbol (see the bottom of p. 44). Thus in this case, identity (5.10) shows that

$$\Big(\frac{A + B\sqrt{m}}{q}\Big) = \Big(\frac{2}{q}\Big)\Big(\frac{A + C\sqrt{m}}{q}\Big),$$

where the symbols on the right hand side are the usual Legendre symbols.

Herbrand's Theorem

My "proof" of Herbrand's Theorem in Chapter 11 is nonsense. The confusion arose because I mixed two possible descriptions of the theorem:

1. You can look at the quotient group $\mathcal{C} = \mathrm{Cl}\,(K)/\mathrm{Cl}\,(K)^p$ (as I did) or the subgroup $\mathrm{Cl}\,(K)[p]$ of ideal classes killed by p; these are $\mathbb{F}_p[G]$-modules.

2. You can consider the whole p-class group $\mathrm{Cl}_p(K)$; in fact, any abelian p-group M of order p^{m+1} is a $\mathbb{Z}_p[G]$-module in a natural way: if $\alpha = a_0 + a_1 p + \ldots + a_m p^m + \ldots \in \mathbb{Z}_p$ (with $0 \leq a_j \leq p-1$), then putting $m^\alpha = m^{a_0 + a_1 p + \ldots + a_m p^m}$ for any $m \in M$ makes M into a $\mathbb{Z}_p[G]$-module.

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

$$\begin{array}{ccc} \mathbb{Z}_p G & \longrightarrow & \mathrm{Aut}\,(M) \\ \big\downarrow{\scriptstyle \pi} & & \big\downarrow \\ \mathbb{F}_p G & \longrightarrow & \mathrm{Aut}\,(M/M^p) \end{array}$$

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

We also have to think about the role of the character ω: when working in $\mathbb{F}_p G$ we simply take $\omega(\sigma_a) = a + p\mathbb{Z} \in \mathbb{F}_p$ and identify $\mathbb{F}_p^\times$ with the roots of unity μ_{p-1}; in $\mathbb{Z}_p G$, we have to lift ω to the Teichmüller character either with Hensel's Lemma or by observing that the sequence a, a^p, a^{p^2}, ... 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 $\mu_{p-1} \subset \mathbb{Z}_p^\times$.

Now the proof of Herbrand's Theorem can be done in either way, but what I did was trying to have the cake and eat it: avoiding the p-adic view and at the same time using the Stickelberger element θ. This cannot possibly work because θ has a p in the denominator which is not much of a nuisance in $\mathbb{Z}_p$ (you simply switch to the quotient field) but is of course a catastrophe in $\mathbb{F}_p$.

Thus in order to save the "proof" given in Chapter 11 one has to

replace	by
$\mathcal{C} = \mathrm{Cl}\,(K)/\mathrm{Cl}\,(K)^p$	$\mathrm{Cl}_p(K)$
$\mathbb{F}_p$	$\mathbb{Z}_p$
cyclotomic ω	Teichmüller ω

The corrected proof will be put on my page along with the rest of Chapter 11.

Additions

Page 20 Teege's first attempt at filling the gap in Legendre's proof was incomplete: see his correction in *Richtigstellung eines früheren Beweises für den Satz, daß es für jede Primzahl p von der Form* $4n+1$ *unendlich viele Primzahlen von der Form* $4n+3$ *gibt, von denen p quadratischer Nichtrest ist und Herleitung des Satzes, daß mindestens eine unter ihnen kleiner als p ist*, Hamb. Mitt. **6** (1924), 100–106. In this paper, Teege also shows that the existence of Gauss's auxiliary prime follows from Legendre's Lemma.

Page 110, Reference [Te1]: The title of Teege's dissertation is *Über die* $\frac{p-1}{2}$*-gliedrigen Gaussischen Perioden in der Lehre von der Kreisteilung und ihre Beziehungen zu anderen Teilen der höheren Arithmetik.*

Page 138: the Davenport-Hasse theorem for Jacobi sums (Cor. 4.33) is actually due to H.H. Mitchell [*On the congruence* $cx^\lambda + 1 \equiv dy^\lambda$ *in a Galois field*, Ann. Math. (2) **18** (1917), 120–131], who expressed the result in terms of cyclotomic numbers.

Page 141: Schwering [728] discusses the quintic power residue character of 2, 3 and 5 as well as the quintic period equation.

Page 170: Another proof of the quadratic reciprocity law in $\mathbb{Z}[i]$ based on Hilbert's genus theory can be found in S. Kuroda [*Über den Dirichletschen Körper*, J. Fac. Sci. Univ. Tokyo, Sect. I **4** (1943), 383–406].

Page 173: Estes & Pall [209] give another proof of Burde's reciprocity law.

Page 200: The version of the quartic reciprocity law (cf. Exercise 6.17) credited to unpublished papers of Gauss and Artin already occurs in Busche [107].

Appendix B: List of Proofs

J. Sochocki, *Bestimmung der constanten Factoren in den Formeln für die lineare Transformation der Thetafunctionen. Die Gauss'schen Summen und das Reciprocitätsgesetz der Legendre'schen Symbole*, Par. Denkschrift, 1878, gives another proof of the quadratic reciprocity law using theta functions.

B. Tangedal gave a proof of the quadratic reciprocity law for Jacobi symbols based on Eisenstein's original proof.

R. Chapman solved the problem of generalizing Nakash's proof that $(5/p) = (p/5)$, giving yet another proof of the quadratic reciprocity law.

Two more proofs were given by ...