MATH. SCAND. 9 (1961), 229–242

REMARKS ON PROOFS BY CYCLOTOMIC FORMULAS OF RECIPROCITY LAWS FOR POWER RESIDUES

TH. SKOLEM

Introduction.

Some classical works of Gauss and Eisenstein contain proofs of the reciprocity laws for power residues based on the theory of cyclotomy. In this paper I intend to expose a slightly modified version of a part of these proofs confining myself first to the quadratic and cubic residues. After that I give a short proof of Eisenstein's reciprocity law [2, p. 78] for l^{th} power residues, l a prime, for brevity only exposed in the case $l=5$. At last I set up a further, perhaps new, proof of the quadratic reciprocity law. In the old proofs I replace a few computational tricks by simple reasoning using the properties of finite fields. The socalled "Ergänzungssätze" are not treated here.

Of fundamental importance in the sequel is the theorem: Let $m \mid q^n - 1$. Then in the finite field K_{q^n} consisting of q^n elements there exist elements a belonging to the exponent m, that is, we have

$$a^m = 1, \quad a^x \neq 1 \qquad \text{for all integers } x \text{ such that } \quad 0 < x < m .$$

Several proofs of this are possible, one of them being just the same as the well known one in elementary number theory set up for the case $n=1$. It is also easily seen that in K_{q^n} there are just $\varphi(m)$ elements a belonging to the exponent m, φ denoting the Euler function.

1.

First I formulate a proof of the quadratic reciprocity law. Let the Legendre symbol (q/p) be $=1$, p and q denoting different natural odd primes. I assert that

$$\left(\frac{(-1)^{\frac{1}{2}(p-1)}}{q}\right) = 1 .$$

Indeed in $K_{q^{\frac{1}{2}(p-1)}}$ there is an element α belonging to the exponent p, because $p \mid q^{\frac{1}{2}(p-1)} - 1$, (q/p) being $\equiv q^{\frac{1}{2}(p-1)} \pmod{p}$. All the roots in $K_{q^{\frac{1}{2}(p-1)}}$ of the equation

$$x^p = 1$$

Received February 2, 1961.

are then $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$, since there are at most p roots. Indeed, we know that in an arbitrary field every algebraic equation of degree n has at most n roots.

Now let $i_1, \ldots, i_{\frac{1}{2}(p-1)}$ be the quadratic residues and $j_1, \ldots, j_{\frac{1}{2}(p-1)}$ the non-residues mod p, and let

$$x_1 = \sum_{r=1}^{\frac{1}{2}(p-1)} \alpha^{i_r}, \quad x_2 = \sum_{s=1}^{\frac{1}{2}(p-1)} \alpha^{j_s}.$$

Then I assert that x_1 and x_2 are the roots of the quadratic equation in $K_{q^{\frac{1}{2}(p-1)}}$

$$x^2 + x + \tfrac{1}{4}\{1 - (-1)^{\frac{1}{2}(p-1)}p\} = 0.$$

Indeed, $x_1 + x_2 + 1 = 1 + \alpha + \ldots + \alpha^{p-1} = 0$ and we may prove $x_1 x_2 = \frac{1}{4}\{1 - (-1)^{\frac{1}{2}(p-1)}p\}$ as follows. If $p \equiv 1 \pmod 4$, we can never have $j_s + i_r \equiv 0 \pmod p$, and obviously the $\left(\frac{1}{2}(p-1)\right)^2$ sums $i_r + j_s$ yield each of the values $1, 2, \ldots, p-1$ just $\frac{1}{4}(p-1)$ times. Hence $x_1 x_2 = \frac{1}{4}(1-p)$. On the other hand, if $p \equiv 3 \pmod 4$, we have $i_r + j_s \equiv 0 \pmod p$ $\frac{1}{2}(p-1)$ times, the remaining $\frac{1}{2}(p-1) \cdot \frac{1}{2}(p-3)$ sums $i_r + j_s$ yielding each of the values $1, \ldots, p-1$ just $\frac{1}{4}(p-3)$ times. Therefore, in this case

$$x_1 x_2 = \tfrac{1}{2}(p-1) - \tfrac{1}{4}(p-3) = \tfrac{1}{4}(1+p).$$

The discriminant is $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = 1 - (1 - (-1)^{\frac{1}{2}(p-1)}p) = (-1)^{\frac{1}{2}(p-1)}p$.

Since q is quadratic residue modulo p, we get

$$x_1{}^q = \left(\sum_{r=1}^{\frac{1}{2}(p-1)} \alpha^{i_r}\right)^q = \sum \alpha^{i_r q} = \sum \alpha^{i_r} = x_1$$

and similarly for x_2, so that x_1 and x_2 belong to the K_q contained in $K_{q^{\frac{1}{2}(p-1)}}$. The elements of K_q can, however, be considered as the rational integers taken modulo q. Thus instead of saying that $(-1)^{\frac{1}{2}(p-1)}p$ is a square in K_q we may say that $(-1)^{\frac{1}{2}(p-1)}p$ is a quadratic residue modulo q, that is

$$\left(\frac{(-1)^{\frac{1}{2}(p-1)}p}{q}\right) = +1.$$

Therefore we have the implications

$$\left(\frac{q}{p}\right) = +1 \Rightarrow \left(\frac{(-1)^{\frac{1}{2}(p-1)}p}{q}\right) = +1,$$

$$\left(\frac{p}{q}\right) = +1 \Rightarrow \left(\frac{(-1)^{\frac{1}{2}(q-1)}q}{p}\right) = +1.$$

This is sufficient for the greater part of the quadratic reciprocity law.

It only remains to prove for $p \equiv q \equiv 3 \pmod 4$ that, if $(q/p) = -1$, then $(p/q) = +1$. By the way, this can be derived from the unsolvability modulo 4 of $x^2 - py^2 - qz^2 = 0$, if one first proves the solvability criterion for $ax^2 + by^2 + cz = 0$ with $(a,b) = (a,c) = (b,c) = 1$. This criterion has earlier been proved by a reduction process due to Lagrange. However, it can be derived easier by a simple use of the box principle as shown independently and almost simultaneously by L. J. Mordell [3] and myself [4]. On the other hand we may prove the implication

$$\left(\frac{q}{p}\right) = -1 \Rightarrow \left(\frac{p}{q}\right) = +1 \quad \text{for} \quad p \equiv q \equiv 3 \pmod 4$$

in a similar way as the implications above. We may consider the field $K_{q^{p-1}}$. Since $p \mid q^{p-1} - 1$, the equation $x^p - 1 = 0$ has again p roots in $K_{q^{p-1}}$, say $1, \alpha, \ldots, \alpha^{p-1}$. We introduce again the two sums x_1 and x_2. Because of $(q/p) = -1$ we obtain

$$x_1^q = x_2, \; x_2^q = x_1 ,$$

so that

$$(x_1 - x_2)^q = x_1^q - x_2^q = x_2 - x_1 .$$

Now there is an element i in $K_{q^{p-1}}$ such that i belongs to the exponent 4, because $4 \mid q^{p-1} - 1$, and we have $i^q = -i$. Hence

$$\big(i(x_1 - x_2)\big)^q = i(x_1 - x_2) ,$$

so that $i(x_1 - x_2)$ is some element of K_q. It can therefore be interpreted as a remainder class of ordinary integers taken modulo q, or in other words we may write

$$i(x_1 - x_2) = r, \qquad r \text{ rational integer} .$$

Hence

$$p = -(x_1 - x_2)^2 \equiv r^2 \pmod q ,$$

whence $(p/q) = +1$.

As the reader will verify, the quadratic reciprocity law is then completely proved.

2.

After this I shall prove, in a similar way, the cubic reciprocity law in the algebraic number field $k\big((-3)^{\frac{1}{2}}\big)$. This law asserts for cubic Legendre symbols that $(l_1/l_2) = (l_2/l_1)$, if l_1 and l_2 are non associated primary primes, that is primes $\equiv -1 \pmod 3$.

I shall make use of some formulas proved in the theory of the equation $x^p = 1$, p natural prime. Letting r be a primitive p^{th} root of 1, $p \equiv 1 \pmod 3$, one puts

$$x_1 = \sum_i r^i, \qquad x_2 = \sum_j r^j, \qquad x_3 = \sum_h r^h,$$

where i runs through those of $1, 2, \ldots, p-1$ which are cubic residues modulo p, j runs through those in one of the two classes of non-residues and h through all belonging to the other class. Then (see [5, p. 351]) the following formulas are valid,

$$(x_1 + \varrho x_2 + \varrho^2 x_3)^3 = p\pi, \qquad (x_1 + \varrho^2 x_2 + \varrho x_3)^3 = p\pi',$$

where $\varrho = \frac{1}{2}(-1 + (-3)^{\frac{1}{2}})$ and π, π' are the primary complex primefactors of p in $k(\varrho)$. I omit here the rather easy proofs of these formulas. I shall consider a finite field K_{q^n}, n such a positive integer that $p \mid q^n - 1$ or in other words n a multiple of the exponent to which q belongs modulo p. If n is chosen as an even number, then not only is $x^p = 1$ solvable in K_{q^n} but an element ϱ exists satisfying $\varrho^2 + \varrho + 1 = 0$. Then the mentioned formulas can be interpreted in K_{q^n}, and they are of course valid there.

The simplest case of the cubic reciprocity law is the case, where l_1 and l_2 are both natural primes $\equiv 2 \pmod 3$. Then we have trivially $(l_1/l_2) = (l_2/l_1) = 1$.

The next case is the one, where l_1 is a natural prime $q \equiv 2 \pmod 3$, while l_2 is a prime factor π of $p = \pi\pi'$, $p \equiv 1 \pmod 3$, $\pi \equiv \pi' \equiv -1 \pmod 3$. First let $(q/\pi) = 1$ in $k(\varrho)$. Then also $(q/\pi') = 1$ and q cubic residue modulo p even in the field k of rationals. Hence in K_{q^n}

$$x_r^q = x_r, \qquad r = 1, 2, 3,$$

whence

$$(x_1 + \varrho x_2 + \varrho^2 x_3)^{q^2} = x_1 + \varrho x_2 + \varrho^2 x_3$$

which shows that

$$\xi_1 = x_1 + \varrho x_2 + \varrho^2 x_3$$

belongs to K_{q^2}. In other words ξ_1 is just one of the remainders mod q in $k(\varrho)$. Then the equation $\xi_1^3 = p\pi$ shows that $p\pi$ is a cubic residue modulo q in $k(\varrho)$ so that $(\pi/q) = 1$, since p is a cubic residue modulo q even in k. Thus it is proved that

$$\left(\frac{q}{\pi}\right) = 1 \Rightarrow \left(\frac{\pi}{q}\right) = 1.$$

Then let $(q/\pi) = \varrho$ in $k(\varrho)$ so that $(q/\pi') = \varrho^2$. Putting

$$q^2 - 1 = 3^m \mu, \qquad 3 \nmid \mu,$$

we have already in the subfield K_{q^2} an element σ which is primitive root of the equation $\sigma^{3^m} = 1$. Outside K_{q^2} but still in K_{q^n}, if n is chosen divis-

ible by 6, we have an element τ such that $\tau^3=\sigma$ because $3^{m+1} \mid q^n-1$, n being divisible by 6. Now I assert that

$$(\xi_1\tau)^{q^2} = \xi_1\tau\,,$$

if we assume the indizes on the "periods" x chosen in such a way that

$$x_1^q = x_2, \qquad x_2^q = x_3, \qquad x_3^q = x_1\,.$$

Indeed

$$\xi_1^q = x_2+\varrho^2x_3+\varrho x_1 = \varrho(x_1+\varrho^2x_2+\varrho x_3) = \varrho\xi_2$$

and similarly $\xi_2^q=\varrho^2\xi_1$ so that

$$\xi_1^{q^2} = \varrho\,\xi_1\,.$$

We may choose σ so that, according as $\mu\equiv 1$ or $2 \pmod 3$, $\sigma^{3^{m-1}}=\varrho^2$ or ϱ. Then $\sigma^{\frac{1}{3}(q^2-1)}=\varrho^2$, and we obtain $(\xi_1\tau)^{q^2}=\xi_1\tau$ as asserted.

This shows that $\xi_1\tau$ belongs to K_{q^2} so that we have in $k(\varrho)$

$$p\pi\sigma \equiv (\xi_1\tau)^3 \pmod q\,,$$

whence, remembering that p is cubic residue $\bmod q$,

$$\left(\frac{\pi\sigma}{q}\right) = 1 \qquad \text{or} \qquad \left(\frac{\pi}{q}\right) = \left(\frac{\sigma}{q}\right)^2,$$

while

$$\left(\frac{\sigma}{q}\right) \equiv \sigma^{\frac{1}{3}(q^2-1)} = \varrho^2\,.$$

Hence $(\pi/q)=\varrho$.

Thus it is proved that $(q/\pi)=\varrho \Rightarrow (\pi/q)=\varrho$. Of course we obtain in the same way

$$\left(\frac{q}{\pi}\right) = \varrho^2 \;\Rightarrow\; \left(\frac{\pi}{q}\right) = \varrho^2,$$

therefore in all cases $(q/\pi)=(\pi/q)$.

Then q may be $\equiv 1 \pmod 3$ and $=\varkappa\varkappa'$, where $\varkappa$ and $\varkappa'$ are $\equiv -1 \pmod 3$, while p is still $\equiv 1 \pmod 3$ and $=\pi\pi'$, $\pi\equiv\pi'\equiv -1 \pmod 3$. Let first $(q/\pi)=1$. Then also $(q/\pi')=1$ and $(q/p)=1$ in k. Hence in K_{q^n}

$$x_1^q = x_1, \qquad x_2^q = x_2, \qquad x_3^q = x_3\,,$$

or in other words x_1, x_2, x_3 belong to K_q. Since $\varrho^q=\varrho$, also ϱ is in K_q. Therefore $\xi_1=x_1+\varrho x_2+\varrho^2x_3$ is in K_q. Further K_q can be interpreted in $k(\varrho)$ as the set of remainder classes $\bmod\varkappa$ and as the set of such classes $\bmod\varkappa'$ as well. Therefore the congruences

$$(x_1+\varrho x_2+\varrho^2x_3)^3 \equiv \pi^2\pi', \qquad (x_1+\varrho^2x+\varrho x_3)^3 \equiv \pi\pi'^2\,,$$

are valid in $k(\varrho)$ modulis $\varkappa$ and $\varkappa'$, that is

$$\left(\frac{\pi^2\pi'}{\varkappa}\right) = \left(\frac{\pi^2\pi'}{\varkappa'}\right) = 1, \qquad \left(\frac{\pi\pi'^2}{\varkappa}\right) = \left(\frac{\pi\pi'^2}{\varkappa'}\right) = 1 .$$

Now let $(q/\pi) = \varrho$. We use again an element τ as above, $\tau^3 = \sigma$, $\sigma^{3^{m-1}} = \varrho, \varrho^2$ according as $\mu \equiv 1, 2 \pmod 3$, putting $q - 1 = 3^m\mu, 3 \nmid \mu$. We may assume that q multiplied by the cubic residues mod p yields the non-residues of the first class. Then

$$\xi_1^q = (x_1 + \varrho x_2 + \varrho^2 x_3)^q = x_2 + \varrho x_3 + \varrho^2 x_1 = \varrho^2 \xi_1 .$$

Hence

$$(\tau\xi_1)^q = \tau^q \varrho^2 \xi_1 = \sigma^{3^{m-1}\mu} \varrho^2 \tau \xi_1 = \tau\xi_1 ,$$

because

$$\sigma^{3^{m-1}\mu} \varrho^2 = \varrho^{\mu^2+2} = 1$$

so that $\tau\xi_1$ belongs to K_q. Since $p\pi\sigma = (\xi_1\tau)^3$, it follows that $p\pi\sigma$ is cubic residue modulis $\varkappa$ and $\varkappa'$ in $k(\varrho)$. Further

$$\left(\frac{\sigma}{\varkappa}\right) \text{ or } \left(\frac{\sigma}{\varkappa'}\right) \equiv \sigma^{\frac{1}{3}(q-1)} \pmod{\varkappa \text{ or } \varkappa'} ,$$

that is

$$\left(\frac{\sigma}{\varkappa}\right) = \left(\frac{\sigma}{\varkappa'}\right) = \varrho .$$

Hence

$$\left(\frac{\pi^2\pi'}{\varkappa}\right) = \varrho^2, \qquad \left(\frac{\pi^2\pi'}{\varkappa'}\right) = \varrho^2,$$

and since $(q/\pi') = \varrho^2$

$$\left(\frac{\pi\pi'^2}{\varkappa}\right) = \left(\frac{\pi\pi'^2}{\varkappa'}\right) = \varrho .$$

If $(q/\pi) = \varrho^2$ we get in the same way

$$\left(\frac{\pi^2\pi'}{\varkappa}\right) = \left(\frac{\pi^2\pi'}{\varkappa'}\right) = \varrho, \qquad \left(\frac{\pi\pi'^2}{\varkappa}\right) = \left(\frac{\pi\pi'^2}{\varkappa'}\right) = \varrho^2 .$$

All these results can be condensed into the equations

$$\left(\frac{\pi^2\pi'}{\varkappa}\right) = \left(\frac{\pi^2\pi'}{\varkappa'}\right) = \left(\frac{q}{\pi}\right)^2 = \left(\frac{q}{\pi'}\right) , \tag{1}$$

$$\left(\frac{\pi\pi'^2}{\varkappa}\right) = \left(\frac{\pi\pi'^2}{\varkappa'}\right) = \left(\frac{q}{\pi'}\right)^2 = \left(\frac{q}{\pi}\right) . \tag{2}$$

Clearly we may exchange the roles of p and q so that we obtain

$$\left(\frac{\varkappa^2\varkappa'}{\pi}\right) = \left(\frac{\varkappa^2\varkappa'}{\pi'}\right) = \left(\frac{p}{\varkappa}\right)^2 = \left(\frac{p}{\varkappa'}\right) , \tag{3}$$

$$\left(\frac{\varkappa\varkappa'^2}{\pi}\right) = \left(\frac{\varkappa\varkappa'^2}{\pi'}\right) = \left(\frac{p}{\varkappa'}\right)^2 = \left(\frac{p}{\varkappa}\right). \tag{4}$$

Multiplication of (2) by $(\varkappa/\pi)$ yields

$$\left(\frac{\pi\pi'^2}{\varkappa}\right)\left(\frac{\varkappa}{\pi}\right) = \left(\frac{q}{\pi}\right)\left(\frac{\varkappa}{\pi}\right) = \left(\frac{\varkappa^2\varkappa'}{\pi}\right)$$

which by (3) is $=(p/\varkappa)^2$ so that

$$\left(\frac{\pi\pi'^2}{\varkappa}\right)\left(\frac{\varkappa}{\pi}\right) = \left(\frac{\pi\pi'^2}{\varkappa}\right)\left(\frac{\pi}{\varkappa}\right),$$

whence $(\varkappa/\pi)=(\pi/\varkappa)$.

Introduction of Jacobi symbols in the usual way makes it possible to derive from what we have proved up to this point the following two more general theorems:

THEOREM 1. *The equation*

$$\left(\frac{L_1}{L_2}\right) = \left(\frac{L_2}{L_1}\right)$$

is valid for any two primary numbers with coprime norms.

THEOREM 2. *If A and B are rational numbers, we have*

$$\left(\frac{A}{B}\right) = 1.$$

I omit here the rather trivial proofs which essentially consist in a multiplying together of Legendre symbols. However I should like to show a very simple proof of the following generalisation of Theorem 1.

THEOREM 3. *We have*

$$\left(\frac{L_1}{L_2}\right) = \left(\frac{L_2}{L_1}\right)$$

for any two coprime primary numbers L_1 and L_2.

PROOF. In order to prove this it suffices to show that $(L'/L)=1$ when L and L' are conjugate and coprime numbers. Letting L be $a+b\varrho$, $a\equiv -1$, $b\equiv 0 \pmod 3$, and making use of Theorems 1 and 2 we get, when $a+b\varrho$ and $a+b\varrho^2$ are coprime,

$$\left(\frac{a+b\varrho^2}{a+b\varrho}\right) = \left(\frac{2a-b}{a+b\varrho}\right), \qquad \left(\frac{b-2a}{a+b\varrho}\right)^2 = \left(\frac{b-2a}{(a+b\varrho)^2}\right) = \left(\frac{(a+b\varrho)^2}{b-2a}\right)$$

$$= \left(\frac{(a^2-b^2+(2a-b)b\varrho}{2a-b}\right) = \left(\frac{a^2-b^2}{2a-b}\right) = 1,$$

so that

$$\left(\frac{2a-b}{a+b\varrho}\right) = 1 .$$

Indeed, $b-2a$ is primary and coprime with the norm of $a+b\varrho$ because a common prime factor would have to divide $(1+2\varrho)a=((-3)^{\frac{1}{2}})a$ and therefore also a and b. Clearly this is sufficient for the proof of Theorem 3, because if the norms of L_1 and L_2 have prime factors in common, the product of the corresponding Legendre symbols will be 1.

By the way it is also possible to prove directly that $(\pi'/\pi)=1$, π primary prime. This can be done by use of the lemma below on the equations

$$\sum_{t=1}^{p-2} t^{\frac{1}{3}(p-1)}(t+1)^{\frac{1}{3}(p-1)} = p\pi, \qquad \sum_{t=1}^{p-2} t^{\frac{1}{3}(2p-1)}(t+1)^{\frac{1}{3}(2p-1)} = p\pi' .$$

Since I have no comments on this proof I only refer to the exposition of it in [1, p. 142).

3.

Then we may look at the 5^{th} power residues in the field $k(\varepsilon)$, $\varepsilon=e^{\frac{1}{5}(2\pi i)}$. Letting p denote a natural prime $\equiv 1 \pmod 5$ and r a primitive p^{th} root of 1, x_1, x_2, x_3, x_4, x_5 may denote the sums $\sum_{i_1} r^{i_1}$, $\sum_{i_2} r^{i_2}$, ..., $\sum_{i_5} r^{i_5}$, where i_1 runs through all 5^{th} power residues of p, i_2 through all residues in a coset to these, i_3, i_4, i_5 respectively through the members of the further cosets. Abbreviating $x_1+\varepsilon x_2+\ldots+\varepsilon^4 x_5$ to (ε,x) we have (see [5, p. 346])

$$(\varepsilon,x)^5 = p\,\psi_1(\varepsilon)\,\psi_2(\varepsilon)\,\psi_3(\varepsilon) \tag{5}$$

besides the analogous equations obtained by replacing ε by ε^2, ε^3, ε^4. Here

$$\psi_1(\varepsilon) = \sum_{t=1}^{p-2} \varepsilon^{\operatorname{ind} t - 2\operatorname{ind}(t+1)}, \qquad \psi_2(\varepsilon) = \sum_{t=1}^{p-2} \varepsilon^{\operatorname{ind} t - 3\operatorname{ind}(t+1)},$$

$$\psi_3(\varepsilon) = \sum_{t=1}^{p-2} \varepsilon^{\operatorname{ind} t - 4\operatorname{ind}(t+1)},$$

where the indizes refer to a primitive number g such that $g^{\frac{1}{5}(p-1)} \equiv \varepsilon$ modulo π_1 say, π_1 being one of the four primefactors in p, $p=\pi_1\pi_2\pi_3\pi_4$. I let $\pi_2=\pi_1(\varepsilon^2)$, $\pi_3=\pi_1(\varepsilon^3)$, $\pi_4=\pi_1(\varepsilon^4)$ when $\pi_1=\pi_1(\varepsilon)$. By the way the number of classes of ideals in $k(\varepsilon)$ is 1.

I shall make use of the lemma: *Let m and n be positive integers $<p-1$. Then*

$$\sum_{t=1}^{p-2} t^m(t+1)^n \equiv 0 \quad \text{or} \quad -\frac{n!}{(m+n-p+1)!\,(p-1-m)!} \pmod p$$

according as $m+n<p-1$ or $\geqq p-1$.

The correctness of this is seen at once by use of the rather trivial theorem that any homogeneous symmetric function of $1,2,\ldots,p-1$ is $\equiv 0 \pmod{p}$, if its degree is $\not\equiv 0 \pmod{p-1}$.

It is obvious that $\psi_1(\varepsilon)$ is $\equiv$

$$\sum_{t=1}^{p-2} t^{\frac{1}{5}(p-1)}(t+1)^{\frac{3}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{3}{5}(p-1)}(t+1)^{\frac{4}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{2}{5}(p-1)}(t+1)^{\frac{1}{5}(p-1)},$$
$$\sum_{t=1}^{p-2} t^{\frac{4}{5}(p-1)}(t+1)^{\frac{2}{5}(p-1)},$$

modulis π_1, π_2, π_3, π_4, respectively. Indeed ε^2, ε^3, ε^4 are $\equiv g^{\frac{1}{5}(p-1)}$ modulis π_2, π_3, π_4, respectively, whence $\varepsilon \equiv g^{\frac{1}{5}(3p-1)}$, $g^{\frac{1}{5}(2p-1)}$, $g^{\frac{1}{5}(4p-1)}$, respectively. According to the lemma, $\psi_1(\varepsilon)$ must be divisible by π_1 and π_3, but not by π_2 or π_4.

In the same manner $\psi_2(\varepsilon)$ is $\equiv$

$$\sum_{t=1}^{p-2} t^{\frac{1}{5}(p-1)}(t+1)^{\frac{2}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{3}{5}(p-1)}(t+1)^{\frac{1}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{2}{5}(p-1)}(t+1)^{\frac{4}{5}(p-1)},$$
$$\sum_{t=1}^{p-2} t^{\frac{4}{5}(p-1)}(t+1)^{\frac{3}{5}(p-1)},$$

modulis π_1, π_2, π_3, π_4, respectively, so that $\psi_2(\varepsilon)$ is divisible by π_1 and π_2, not by π_3 or π_4.

Finally $\psi_3(\varepsilon)$ is $\equiv$

$$\sum_{t=1}^{p-2} t^{\frac{1}{5}(p-1)}(t+1)^{\frac{1}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{3}{5}(p-1)}(t+1)^{\frac{3}{5}(p-1)}, \quad \sum_{t=1}^{p-2} t^{\frac{2}{5}(p-1)}(t+1)^{\frac{2}{5}(p-1)},$$
$$\sum_{t=1}^{p-2} t^{\frac{4}{5}(p-1)}(t+1)^{\frac{4}{5}(p-1)},$$

modulis π_1, π_2, π_3, π_4, respectively. Thus $\psi_3(\varepsilon)$ is divisible by π_1 and π_3, but not by π_2 or π_4.

Hence (5) yields

$$(\varepsilon, x)^5 = E(\varepsilon)\pi_1^4\pi_2^2\pi_3^3\pi_4,$$

where $E(\varepsilon)$ is a unit in $k(\varepsilon)$. Replacing ε by ε^2, ε^3, ε^4 we get analogous equations

$$(\varepsilon^2, x)^5 = E(\varepsilon^2)\pi_2^4\pi_4^2\pi_1^3\pi_3, \quad (\varepsilon^3, x)^5 = E(\varepsilon^3)\pi_3^4\pi_1^2\pi_4^3\pi_2,$$
$$(\varepsilon^4, x)^5 = E(\varepsilon^4)\pi_4^4\pi_3^2\pi_2^3\pi_1.$$

A number in $k(\varepsilon)$, not divisible by $1-\varepsilon$, is said to be *semiprimary*, if it is $\equiv$ a rational number $\bmod (1-\varepsilon)^2$. Since the remainders of the numbers $\not\equiv 0 \pmod{1-\varepsilon}$ are 1, 2, 3, 4 multiplied by 1, ε, ε^2, ε^3, ε^4, it is clear that every integer in $k(\varepsilon)$ can be multiplied by such a power of ε

that the product becomes semiprimary. Therefore we may assume π_1, chosen above, semiprimary. Then also π_2, π_3, π_4 will be semiprimary because all the numbers $1-\varepsilon^i$, $i=1,2,3,4$, are associated, and π_1, π_2, π_3, π_4 all $\equiv$ the same rational integer modulo $(1-\varepsilon)^2$. Hence $\pi_1{}^4\pi_2{}^2\pi_3{}^3\pi_4$ and the analogous products must be $\equiv \pm 1 \pmod{(1-\varepsilon)^2}$. Further

$$(\varepsilon,x)^5 \equiv x_1{}^5+x_2{}^5+\ldots+x_5{}^5 \equiv (x_1+x_2+\ldots+x_5)^5 \equiv -1 \pmod 5 .$$

Multiplication of the first and the fourth of our equations yields

$$(\varepsilon,x)^5(\varepsilon^4,x)^5 = E(\varepsilon)E(\varepsilon^4)(\pi_1\pi_2\pi_3\pi_4)^5 .$$

Here $\pi_1\pi_2\pi_3\pi_4 = \text{norm } \pi_1 = p$. It is easily shown that $(\varepsilon,x)(\varepsilon^4,x)=p$ (see [5, p. 346]). Therefore $E(\varepsilon)E(\varepsilon^4)=1$. In the theory of cyclotomy a very elegant proof is found (see [1, p. 269]), that if $F(\varepsilon)F(\varepsilon^{-1})=1$, then $F(\varepsilon)$ is some power of ε. However, this follows as well from a general theorem in the theory of algebraic number fields. Thus $E(\varepsilon)=\pm\varepsilon^a$ which yields

$$(\varepsilon,x)^5 = \pm\varepsilon^a\pi_1{}^4\pi_2{}^2\pi_3{}^3\pi_4, \qquad a = 0,1,2,3, \text{ or } 4 .$$

Modulo $(1-\varepsilon)^2$ the left hand side is $\equiv -1$ while the right side is $\equiv \pm\varepsilon^a$. It follows that $a=0$ so that the equation can be simplified to

$$(\varepsilon,x)^5 = \pm\,\pi_1{}^4\pi_2{}^2\pi_3{}^3\pi_4 .$$

I shall now prove that the Legendre symbols (q/π) and (π/q) are equal, q a rational prime $\neq 5$, π a semiprimary prime in $k(\varepsilon)$ coprime with 5 and q. I distinguish three cases of which the two first are very simple.

1° The prime π is of degree 4. Then $\pi=pE$, p rational prime $\equiv 2$ or $3 \pmod 5$, E a semiprimary unit. It is easy to prove that the semiprimary units are just those in the quadratic subfield $k(5^{\frac{1}{2}})$. Therefore π belongs to $k(5^{\frac{1}{2}})$ so that it is unchanged by the automorphism $\varepsilon \to \varepsilon^{-1}$. Now, because $5 \mid p^2+1$ and $q^{p-1}\equiv 1 \pmod{\pi \text{ or } p}$, we have

$$\left(\frac{q}{\pi}\right) \equiv q^{\frac{1}{5}(p^4-1)} \equiv 1 \pmod\pi . \qquad \text{Thus} \quad \left(\frac{q}{\pi}\right) = 1 .$$

On the other hand we may write $(\pi/q)=\varepsilon^a$, a one of the numbers 0, 1, 2, 3, 4. Applying the automorphism $\varepsilon \to \varepsilon^{-1}$ we obtain $(\pi/q)=\varepsilon^{-a}$. Hence $a=0$, whence $(\pi/q)=1$.

2° The degree of π is 2. If p is the natural prime $\equiv 4 \pmod 5$ divisible by π, then $p=\pi\pi'$, where π' is a semiprimary prime conjugate to π. Then again the automorphism $\varepsilon \to \varepsilon^{-1}$ leaves π and π' unchanged. Because $5 \mid p+1$ we get

$$\left(\frac{q}{\pi}\right) \equiv q^{\frac{1}{5}(p^2-1)} \equiv 1, \qquad \text{that is} \quad \left(\frac{q}{\pi}\right) = 1 .$$

On the other hand $(\pi/q)=1$ for the same reason as before.

3° The degree of π is 1. Then for some natural prime $p \equiv 1 \pmod 5$ we have, writing π_1 instead of π,

$$p = \pi_1\pi_2\pi_3\pi_4, \qquad \text{where} \quad \pi_i = \pi_1(\varepsilon^i), \quad i = 1,2,3,4\,,$$

and $\pi_1, \pi_2, \pi_3, \pi_4$ are semiprimary. I consider the field K_{q^n}, where n shall be a common multiple of 4 and $p-1$. Then the equations $x^p - 1$ and $x^5 - 1 = 0$ have primitive roots r and ε in K_{q^n}. Therefore elements defined as x_1, x_2, x_3, x_4, x_5 above exist in this field, and we have the equation

$$(\varepsilon,x)^5 = \pm \pi_1^4\pi_2^2\pi_3^3\pi_4 \tag{6}$$

together with the analogous ones.

Now let $(q/\pi) = 1$. Then, in K_{q^n}

$$x_i^q = x_i, \qquad i = 1,2,3,4,5\,.$$

Letting f be the least positive integer such that $q^f \equiv 1 \pmod 5$ we therefore obtain

$$(\varepsilon,x)^{q^f} = (\varepsilon,x)\,,$$

which shows that (ε,x) is an element of K_{q^f}. Now K_{q^f} is just the field of remainder classes modulo q in $k(\varepsilon)$. Then (6) shows that $\pi_1^4\pi_2^2\pi_3^3\pi_4$ is a 5^{th} power residue modulo q in $k(\varepsilon)$. Thus we may write

$$\left(\frac{\pi_1^4\pi_2^2\pi_3^3\pi_4}{q}\right) = 1\,.$$

However it is clear by consideration of automorphisms that

$$\left(\frac{\pi_i}{q}\right) = \left(\frac{\pi_1}{q}\right)^i, \qquad i = 1,2,3,4\,.$$

This inserted in (6) yields $(\pi_1/q) = 1$, and thus the assertion.

Then let $(q/\pi) = \varepsilon$. We may assume the indizes for the x_i chosen in such a way that in K_{q^n}

$$x_1^q = x_2, \quad x_2^q = x_3, \quad x_3^q = x_4, \quad x_4^q = x_5, \quad x_5^q = x_1\,.$$

Then the reader will verify that

$$(\varepsilon,x)^{q^f} = \varepsilon^{-fq^f}(\varepsilon^{q^f},x) = \varepsilon^{-f}(\varepsilon,x)\,.$$

In K_{q^f} there is an element σ which is primitive root of the equation

$$\sigma^{5^m} = 1, \qquad \text{when} \quad q^f - 1 = 5^m\mu, \quad 5 \nmid \mu\,.$$

We may choose σ so that

$$\sigma^{5^{m-1}} = \varepsilon^{f\mu^{-1}}\,.$$

Outside K_{q^f}, but still in K_{q^n}, there is a τ such that

$$\tau^5 = \sigma .$$

Indeed $5^{m+1} \mid q^n - 1$ because n is, according to supposition, divisible by 20 and $q^{20} - 1 = (q^4-1)(q^{16}+q^{12}+q^8+q^4+1)$ with $q^f - 1$ a factor of $q^4 - 1$ in any case. We obtain now, since $\tau^{q^f-1} = \sigma^{5^{m-1}\mu} = \varepsilon^f$,

$$\big(\tau(\varepsilon,x)\big)^{q^f} = \tau\varepsilon^f(\varepsilon,x)^{q^f} = \tau(\varepsilon,x) .$$

Thus $\tau(\varepsilon,x)$ is a remainder class modulo q in $k(\varepsilon)$. Further

$$\big(\tau(\varepsilon,x)\big)^5 = \pm\, \pi_1{}^4\pi_2{}^2\pi_3{}^3\pi_4\sigma \pmod{q} .$$

This furnishes in the same way as above

$$\left(\frac{\pi_1\sigma}{q}\right) = 1 \qquad \text{or} \qquad \left(\frac{\pi_1}{q}\right) = \left(\frac{\sigma}{q}\right)^{-1} .$$

Now if $\varkappa$ is any prime divisor of q in $k(\varepsilon)$

$$\left(\frac{\sigma}{\varkappa}\right) = \sigma^{\frac{1}{5}(q^f-1)} = \sigma^{5^{m-1}\mu} = \varepsilon^f .$$

Letting g be the number of different primes in $k(\varepsilon)$ dividing q we have $fg = 4$ and therefore

$$\left(\frac{\sigma}{q}\right) = \varepsilon^{fg} = \varepsilon^4 ,$$

so that $(\pi_1/q) = \varepsilon$, and the assertion is proved.

It follows by multiplication of symbols (q/π) and (π/q), respectively, that more generally

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\beta}{\alpha}\right)$$

for arbitrary rational integer a and an arbitrary primary β in $k(\varepsilon)$, provided that 5, a and β are mutually coprime. This is Eisenstein's Reciprocity Law (see [2, p. 78]).

I think the reader will understand that it is possible to extend these considerations to higher power residues. Only the existence of more than one class of ideals in some cyclotomic fields makes a little trouble. An eventual treatment of these more complicated cases must be postponed.

4.

At last I give a proof of the quadratic law of reciprocity in k which does not apply the Lagrange resolvents used in the theory of cyclotomy. Indeed it suffices to use the trivial formula

$$p = \prod_{h=1}^{p-1} (1-r^h) , \tag{7}$$

where r is a primitive root of the equation $x^p = 1$. I consider a field K_{q^n}, n a multiple of $p-1$. There is then an element r in this field which belongs to the exponent p and (7) is valid.

Firstly let p be $\equiv 3 \pmod 4$. Then I assert that

$$p = -\prod_j (1-r^j)^2 , \tag{8}$$

where j runs through the quadratic residues mod p. Indeed (7) can be written $p = \prod_j (1-r^j) \prod_j (1-r^{-j})$, j running through all quadratic residues modulo p, since $-j$ then runs through all non residues. However

$$\prod_j (1-r^{-j}) = (-1)^{\frac{1}{2}(p-1)} \prod_j r^{-j}(1-r^j) ,$$

so that we obtain (8) because $\sum j \equiv 1^2 + 2^2 + \ldots + \left(\tfrac{1}{2}(p-1)\right)^2 \equiv 0 \pmod p$. Now let $(q/p) = +1$ in k. Then in K_{q^n}

$$\prod_j (1-r^j)^q = \prod_j (1-r^{qj}) = \prod_j (1-r^j) ,$$

because qj again runs through the quadratic residues. Therefore $\prod_j (1-r^j)$ belongs to K_q which is the set of remainder classes modulo q in k. Thus in k we have according to (8)

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{1}{2}(q-1)} .$$

Then let $(q/p) = -1$. In this case

$$\prod_j (1-r^j)^q = \prod_j (1-r^{qj}) = \prod_j (1-r^{-j}) = (-1)^{\frac{1}{2}(p-1)} \prod_j (1-r^j) ,$$

that is $\prod_j (1-r^j)^q = -\prod_j (1-r^j)$. Therefore $\prod_j (1-r^j)$ is not an element of K_q so that, according to (8), $-p$ is not a square in K_q, or in other words

$$\left(\frac{-p}{q}\right) = -1 \qquad \text{or} \qquad \left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(q+1)} .$$

Secondly, let p be $\equiv 1 \pmod 4$. Understanding by g a primitive number modulo p it is easy to verify that instead of (7) we may write

$$p = P^2 Q^2 , \tag{9}$$

where

$$P = (r-r^{-1})(r^{g^2} - r^{-g^2})(r^{g^3} - r^{-g^3}) \ldots (r^{g^{\frac{1}{2}(p-5)}} - r^{-g^{\frac{1}{2}(p-5)}})$$

and

$$Q = (r^g - r^{-g})(r^{g^3} - r^{-g^3}) \ldots (r^{g^{\frac{1}{2}(p-3)}} - r^{-g^{\frac{1}{2}(p-3)}}) .$$

Now let $(q/p)=+1$, say $q\equiv g^{2s} \pmod{p}$. Then in K_{q^n}

$$P^q = (r^{g^{2s}}-r^{-g^{2s}})(r^{g^{2s+2}}-r^{-g^{2s+2}}) \ldots (r^{g^{2s+\frac{1}{2}(p-5)}}-r^{-g^{2s+\frac{1}{2}(p-5)}}) = (-1)^s P .$$

Indeed the first $\frac{1}{4}(p-1)-s$ factors in the expression for P^q also occur in P, whereas each of the last s factors in P^q occurs in P with opposite sign. Similarly $Q^q=(-1)^s Q$. Hence

$$(PQ)^q = PQ$$

which means that PQ is an element of K_q. Then (9) shows that p is a square in K_q, that is, $(p/q)=+1$.

Then let $(q/p)=-1$, say $q\equiv g^{2s+1} \pmod{p}$. Then one observes in the same manner that

$$P^q = (-1)^s Q, \qquad Q^q = (-1)^{s+1} P ,$$

so that

$$(PQ)^q = -PQ .$$

This means that PQ is not in K_q so that, according to (9), p is not a square in K_q, that is, $(p/q)=-1$.

Collecting the obtained results the reader will convince himself that the quadratic reciprocity law in the natural number field is completely proved.

REFERENCES

1. P. Bachmann, *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie*, Leipzig, 1872.
2. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, II, *Reziprozitätsgesetz*. Jber. Deutsche Math. Verein, Ergänzungsbd. 6 (1930).
3. L. J. Mordell, *On the equation* $ax^2+by^2-cz^2=0$, Monatsh. Math. Phys. 55 (1951), 323–327.
4. Th. Skolem, *A simple proof of the condition of solvability of the diophantine equation* $ax^2+by^2+cz^2=0$, Norske Vid. Selsk. Forh. Trondheim 24 (1951), 102–107.
5. H. Weber, *Kleines Lehrbuch der Algebra*, Braunschweig, 1912.

UNIVERSITY OF OSLO, NORWAY