H.W. Lenstra, Jr.
Department of Mathematics # 3840, University of California, Berkeley, CA 94720–3840, U.S.A.
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
hwl@math.berkeley.edu, hwl@math.leidenuniv.nl

P. Stevenhagen
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
psh@math.leidenuniv.nl

Artin reciprocity and

Emil Artin was born on March 3, 1898 in Vienna, as the son of an art dealer and an opera singer, and he died on December 20, 1962 in Hamburg. He was one of the founding fathers of modern algebra. Van der Waerden acknowledged his debt to Artin and to Emmy Noether (1882–1935) on the title page of his *Moderne Algebra* (1930–31), which indeed was originally conceived to be jointly written with Artin. The single volume that contains Artin's collected papers, published in 1965 [1], is one of the other classics of twentieth century mathematics.

Artin's two greatest accomplishments are to be found in algebraic number theory. Here he introduced the *Artin L-functions* (1923) [2], which are still the subject of a major open problem, and he formulated (1923) [2] and proved (1927) [3] *Artin's reciprocity law*, to which the present paper is devoted.

Artin's reciprocity law is one of the cornerstones of *class field theory*. This branch of algebraic number theory was during the pre-war years just as forbidding to the mathematical public as modern algebraic geometry was to be in later years. It is still not the case that the essential simplicity of class field theory is known to "any arithmetician from the street" [16]. There is indeed no royal road to class field theory, but, as we shall show, a complete and rigorous statement of Artin's reciprocity law is not beyond the scope of a first introduction to the subject. To illustrate its usefulness in elementary number theory, we shall apply it to prove a recently observed property of Mersenne primes.

The Frobenius map

The identity

$$(a+b)^2 = a^2 + 2ab + b^2$$

can be appreciated by anybody who can add and multiply. Thus, the modern mathematician may be inclined to view it as belonging to the discipline that studies addition and multiplication—that is, to *ring theory*. In this paper, we suppose all rings to be *commutative* and to have a unit element 1. With this convention, the identity above is a simple consequence of the ring axioms, if the factor 2 in $2ab$ is interpreted as $1+1$. It takes an especially simple form if the term $2ab$ drops out:

$$(a+b)^2 = a^2 + b^2 \qquad \text{if } 2 = 0.$$

Likewise, the general ring-theoretic identity

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

(where $3 = 1+1+1$) assumes the simple form

$$(a+b)^3 = a^3 + b^3 \qquad \text{if } 3 = 0.$$

One may now wonder: if n is *any* positive integer, does one have

$$(a+b)^n = a^n + b^n \qquad \text{if } n = 0?$$

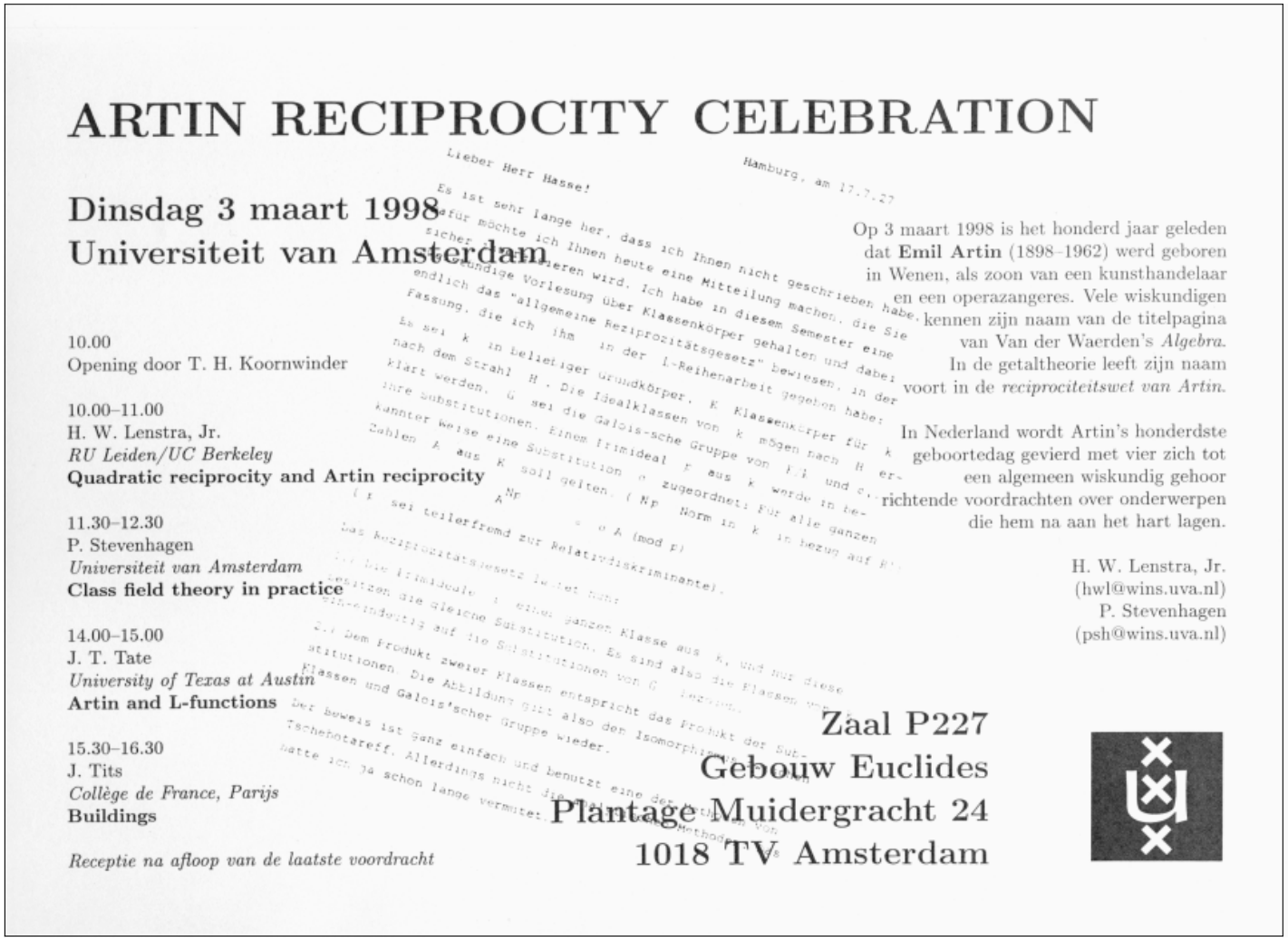
This fails already for the very next value of n: in the ring $\mathbf{Z}/4\mathbf{Z}$ of integers modulo 4, in which 4 equals 0, one has $(1+1)^4 = 16 = 0$ but $1^4 + 1^4 = 2 \neq 0$. One can show that it actually fails for *any* $n > 1$ that is composite. However, if n is *prime* then the statement is correct. To prove it, one observes that for any prime number n and any positive integer $i < n$ the number $i!(n-i)!\binom{n}{i} = n!$ is divisible by n, while $i!(n-i)!$ is not, so that $\binom{n}{i}$ must be divisible by n; hence in a ring with $n = 0$ the only terms in the expansion $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$ that remain are those with $i = 0$ or $i = n$.

The result just proved admits an attractive algebraic reformulation. Write p instead of n, in order to emphasize that we restrict to prime numbers. Let R be a ring in which one has $p = 0$, and define the pth power map $F\colon R \to R$ by $F(x) = x^p$. We just proved the identity

$$F(a+b) = F(a) + F(b),$$

that is, F "respects addition". Since the commutative law implies $(ab)^p = a^p b^p$, it respects multiplication as well. Finally, it respects the unit element: $F(1) = 1$. These three properties constitute

Mersenne primes



ARTIN RECIPROCITY CELEBRATION

Dinsdag 3 maart 1998
Universiteit van Amsterdam

10.00
Opening door T. H. Koornwinder

10.00–11.00
H. W. Lenstra, Jr.
RU Leiden/UC Berkeley
Quadratic reciprocity and Artin reciprocity

11.30–12.30
P. Stevenhagen
Universiteit van Amsterdam
Class field theory in practice

14.00–15.00
J. T. Tate
University of Texas at Austin
Artin and L-functions

15.30–16.30
J. Tits
Collège de France, Parijs
Buildings

Receptie na afloop van de laatste voordracht

Op 3 maart 1998 is het honderd jaar geleden dat **Emil Artin** (1898–1962) werd geboren in Wenen, als zoon van een kunsthandelaar en een operazangeres. Vele wiskundigen kennen zijn naam van de titelpagina van Van der Waerden's *Algebra*. In de getaltheorie leeft zijn naam voort in de *reciprociteitswet van Artin*.

In Nederland wordt Artin's honderdste geboortedag gevierd met vier zich tot een algemeen wiskundig gehoor richtende voordrachten over onderwerpen die hem na aan het hart lagen.

H. W. Lenstra, Jr.
(hwl@wins.uva.nl)
P. Stevenhagen
(psh@wins.uva.nl)

Zaal P227
Gebouw Euclides
Plantage Muidergracht 24
1018 TV Amsterdam

On March 3, 1998, the centenary of Emil Artin was celebrated at the Universiteit van Amsterdam. The present paper is based on the two morning lectures. The announcement incorporated part of a letter from Artin to Hasse, reproduced from [9, p. 31].

the definition of a *ring homomorphism*, which leads to the following reformulation.

Theorem 1. *Let p be a prime number and R a ring in which we have $p = 0$. Then the pth power map $R \to R$ is a ring homomorphism from R to itself.*

The map in the theorem is called the *Frobenius map*, after Georg Ferdinand Frobenius (1849–1917), who realized its importance in algebraic number theory in 1880 (see [10, 15]).

Many "reciprocity laws", including Artin's, help answering the question: *which* ring homomorphism $R \to R$ is F? That is, does F have a more direct description than through pth powering? We give two examples in which this can be done. Throughout, we let p be a prime number.

The simplest non-zero ring with $p = 0$ is the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ of integers modulo p. Since any element of $\mathbf{F}_p$ can be written as $1 + 1 + \ldots + 1$, the only ring homomorphism $\mathbf{F}_p \to \mathbf{F}_p$ is the identity. In particular, the Frobenius map $F\colon \mathbf{F}_p \to \mathbf{F}_p$ is the identity. Looking at the definition of F, we see that we proved *Fermat's little theorem*: for any integer a, one has $a^p \equiv a \bmod p$.

Next we consider quadratic extensions of $\mathbf{F}_p$. Let d be a non-zero integer, and let p be a prime number not dividing $2d$. We consider the ring $\mathbf{F}_p[\sqrt{d}]$, the elements of which are by definition the formal expressions $u + v\sqrt{d}$, with u and v ranging over $\mathbf{F}_p$. No two of these expressions are considered equal, so the number of elements of the ring equals p^2. The ring operations are the obvious ones suggested by the notation; that is, one defines

$$\begin{aligned}(u + v\sqrt{d}) + (u' + v'\sqrt{d}) &= (u + u') + (v + v')\sqrt{d},\\ (u + v\sqrt{d}) \cdot (u' + v'\sqrt{d}) &= (uu' + vv'd) + (uv' + vu')\sqrt{d},\end{aligned}$$

where d in $vv'd$ is interpreted to be the element $(d \bmod p)$ of $\mathbf{F}_p$. It is straightforward to show that with these operations $\mathbf{F}_p[\sqrt{d}]$ is indeed a ring with $p = 0$.

Let us now apply the Frobenius map F to a typical element $u + v\sqrt{d}$. Using, in succession, the definition of F, the fact that it is a ring homomorphism, Fermat's little theorem, the defining relation $(\sqrt{d})^2 = d$, and the fact that p is odd, we find

$$F(u + v\sqrt{d}) = (u + v\sqrt{d})^p = u^p + v^p(\sqrt{d})^p = u + vd^{(p-1)/2}\sqrt{d}.$$

This leads us to investigate the value of $d^{(p-1)/2}$ in $\mathbf{F}_p$. Again from Fermat's little theorem, we have

$$0 = d^p - d = d \cdot (d^{(p-1)/2} - 1) \cdot (d^{(p-1)/2} + 1).$$

Since $\mathbf{F}_p$ is a field, one of the three factors d, $d^{(p-1)/2} - 1$, $d^{(p-1)/2} + 1$ must vanish. As p does not divide $2d$, it is exactly one of the last two. The *quadratic residue symbol* $(\frac{d}{p})$ distinguishes between the two cases: for $d^{(p-1)/2} = +1$ in $\mathbf{F}_p$ we put $(\frac{d}{p}) = +1$, and for $d^{(p-1)/2} = -1$ we put $(\frac{d}{p}) = -1$. The conclusion is that the Frobenius map is one of the two "obvious" automorphisms of $\mathbf{F}_p[\sqrt{d}]$: for $(\frac{d}{p}) = +1$ it is the identity, and for $(\frac{d}{p}) = -1$ it is the map sending $u + v\sqrt{d}$ to $u - v\sqrt{d}$.

The assignment $u + v\sqrt{d} \mapsto u - v\sqrt{d}$ is clearly reminiscent of complex conjugation, and it defines an automorphism in more general circumstances involving square roots. For example, define a ring $\mathbf{Q}[\sqrt{d}]$ by simply replacing $\mathbf{F}_p$ with the field $\mathbf{Q}$ of rational numbers in the above. The ring $\mathbf{Q}[\sqrt{d}]$ is a field when d is not a perfect square; but whether or not it is a field, it has an identity automorphism as well as an automorphism of order 2 that maps $u + v\sqrt{d}$ to $u - v\sqrt{d}$. If we restrict to integral u and v, and reduce modulo p, then one of these two automorphisms gives rise to the Frobenius map of $\mathbf{F}_p[\sqrt{d}]$.

The Artin symbol

We next consider higher degree extensions. Instead of $X^2 - d$, we take any polynomial $f \in \mathbf{Z}[X]$ of positive degree n and with leading coefficient 1. Instead of $d \neq 0$, we require that f not have repeated factors or, equivalently, that its discriminant $\Delta(f)$ be non-zero. Instead of $\mathbf{F}_p[\sqrt{d}]$, for a prime number p, we consider the ring $\mathbf{F}_p[\alpha]$ consisting of all p^n formal expressions

$$u_0 + u_1\alpha + u_2\alpha^2 + \ldots + u_{n-1}\alpha^{n-1}$$

with coefficients $u_i \in \mathbf{F}_p$, the ring operations being the natural ones with $f(\alpha) = 0$. Here the coefficients of f, which are integers, are interpreted in $\mathbf{F}_p$, as before. (Formally, one may define $\mathbf{F}_p[\alpha]$ to be the quotient ring $\mathbf{F}_p[Y]/f(Y)\mathbf{F}_p[Y]$.) In the same manner, replacing $\mathbf{F}_p$ with $\mathbf{Q}$, we define the ring $\mathbf{Q}[\alpha]$. It is a field if and only if f is irreducible, but there is no reason to assume that this is the case.

Note that we use the same symbol α for elements of different rings. This is similar to the use of the symbols 0, 1, $2 = 1 + 1$ for elements of different rings, and just as harmless.

We now need to make an important assumption, which is automatic for $n \leq 2$ but not for $n \geq 3$. Namely, instead of two automorphisms, we assume that a finite *abelian* group G of ring automorphisms of $\mathbf{Q}[\alpha]$ is given such that we have an equality

$$f = \prod_{\sigma \in G} \big(X - \sigma(\alpha)\big)$$

of polynomials with coefficients in $\mathbf{Q}[\alpha]$; in particular, the order of G should be n. The existence of G is a strong assumption. For example, in the important case that f is irreducible it is equivalent to $\mathbf{Q}[\alpha]$ being a Galois extension of $\mathbf{Q}$ with an abelian Galois group.

Just as in the quadratic case, the Frobenius map of $\mathbf{F}_p[\alpha]$ is for almost all p induced by a unique element of the group G. The precise statement is as follows.

Theorem 2. *Let the notation and hypotheses be as above, and let p be a prime number not dividing $\Delta(f)$. Then there is a unique element $\varphi_p \in G$ such that the Frobenius map of the ring $\mathbf{F}_p[\alpha]$ is the "reduction" of φ_p modulo p, in the following sense: in the ring $\mathbf{Q}[\alpha]$, one has*

$$\alpha^p = \varphi_p(\alpha) + p \cdot (q_0 + q_1\alpha + \ldots + q_{n-1}\alpha^{n-1})$$

for certain rational numbers $q_0, \ldots, q_{n-1}$ of which the denominators are not divisible by p.

In all our examples, the condition on the denominators of the q_i is satisfied simply because the q_i are integers, in which case α^p and $\varphi_p(\alpha)$ are visibly "congruent modulo p". However, there are cases in which the coefficients of $\varphi_p(\alpha)$ have a true denominator, so that the q_i will have denominators as well. Requiring the latter to not be divisible by p prevents us from picking *any* $\varphi_p \in G$ and just *defining* the q_i by the equation in the theorem.

The proof of the theorem is a mildly technical exercise in ring theory, and we suppress it here. It involves no number-theoretic

subtleties of any kind, and one should not think of the theorem as a deep one. The assumption that G be abelian cannot be omitted.

The element φ_p of G is referred to as the *Artin symbol* of p. In the case $n = 2$ it is virtually identical to the quadratic symbol $(\frac{\Delta(f)}{p})$. Note that for $f = X^2 - d$ we have $\Delta(f) = 4d$, so the condition that p not divide $\Delta(f)$ is in this case equivalent to p not dividing $2d$.

We can now say that, for the rings $\mathbf{F}_p[\alpha]$ occurring in Theorem 2, knowing the Frobenius map is equivalent to knowing the Artin symbol φ_p in the group G. The Artin reciprocity law imposes strong restrictions on how φ_p varies over G as p ranges over all prime numbers not dividing $\Delta(f)$, and in this way it helps in determining the Frobenius map. Let us consider an example.

Take $f = X^3 + X^2 - 2X - 1$, an irreducible polynomial with discriminant $\Delta(f) = 49 = 7^2$. Since the discriminant is a square, Galois theory predicts that we are able to find a group G as in the theorem. Indeed, our ring $\mathbf{Q}[\alpha]$—a field, actually—turns out to have an automorphism σ with

$$\sigma(\alpha) = \alpha^2 - 2,$$

and an automorphism $\tau = \sigma^2$ with

$$\tau(\alpha) = \sigma(\sigma(\alpha)) = (\alpha^2 - 2)^2 - 2 = -\alpha^2 - \alpha + 1;$$

here we used the defining relation $f(\alpha) = 0$, that is, $\alpha^3 = -\alpha^2 + 2\alpha + 1$. One checks that σ and τ constitute, together with the identity automorphism 1, a group of order 3 that satisfies the condition $f = (X - \alpha)(X - \sigma(\alpha))(X - \tau(\alpha))$ stated before Theorem 2.

Let us compute some of the Artin symbols φ_p for primes $p \neq 7$. We have

$$\alpha^2 \equiv \alpha^2 - 2 = \sigma(\alpha) \bmod 2,$$

so $\varphi_2 = \sigma$. Likewise,

$$\alpha^3 = -\alpha^2 + 2\alpha + 1 \equiv -\alpha^2 - \alpha + 1 = \tau(\alpha) \bmod 3,$$

so $\varphi_3 = \tau$. A small computation yields

$$\alpha^5 = -4\alpha^2 - 5\alpha + 3 \equiv \alpha^2 - 2 = \sigma(\alpha) \bmod 5,$$

so $\varphi_5 = \sigma$. Continuing in this way, one can list the value of φ_p for a few small p.

p	2	3	5	11	13	17	19	23
φ_p	σ	τ	σ	τ	1	τ	σ	σ
p	29	31	37	41	43	47	53	59
φ_p	1	τ	σ	1	1	σ	τ	τ
p	61	67	71	73	79	83	89	97
φ_p	σ	τ	1	τ	σ	1	σ	1

This table can easily be made with a computer, but that is not what we did. Instead, we applied Artin's reciprocity law. There is an easy pattern in the table, which the reader may enjoy finding before reading on.

Artin symbols are worth knowing because they control much of the arithmetic of $\mathbf{Q}[\alpha]$. They tell us in which way the polynomial f with $f(\alpha) = 0$ factors modulo the prime numbers coprime to $\Delta(f)$. This gives strong information about the prime ideals of the ring $\mathbf{Z}[\alpha]$, which for $\mathbf{Z}[\alpha]$ are just as important as the prime numbers themselves are for $\mathbf{Z}$. Here are two illustrative results. Let the situation again be as in the theorem.

Result 1. *The degree of each irreducible factor of the polynomial $(f \bmod p)$ in $\mathbf{F}_p[X]$ is equal to the order of φ_p in the group G. In particular, one has $\varphi_p = 1$ in G if and only if $(f \bmod p)$ splits into n linear factors in $\mathbf{F}_p[X]$.*

It is, for $n > 2$, quite striking that all irreducible factors of $(f \bmod p)$ have the *same* degree. This exemplifies the strength of our assumptions. In the case $n = 2$, Result 1 implies that one has $(\frac{d}{p}) = 1$ if and only if d is congruent to a square modulo p, a criterion that is due to Euler (1755).

Result 2. *The polynomial f is irreducible in $\mathbf{Z}[X]$ if and only if G is generated by the elements φ_p, as p ranges over all prime numbers not dividing $\Delta(f)$.*

The first result is "local" in the sense that it considers a single prime number p, but the second one is global: it views the totality of all p. Result 1 and the 'if'-part of Result 2 belong to algebra and are fairly straightforward. The 'only if'-part of Result 2 is harder: it is number theory. For example, Result 2 implies that an integer d is not a square if and only if there exists a prime number p with $(\frac{d}{p}) = -1$.

Amusingly, there is also an Artin symbol that "imitates" complex conjugation just as φ_p imitates the Frobenius map. We denote it by φ_{-1}; it is the unique element of G with the property that every ring homomorphism λ from $\mathbf{Q}[\alpha]$ to the field of complex numbers maps $\varphi_{-1}(\alpha)$ to the complex conjugate of $\lambda(\alpha)$. As in Result 1, the degree of each irreducible factor of f over the field $\mathbf{R}$ of real numbers equals the order of φ_{-1} in G, which is 1 or 2. The case $f = X^2 - d$ again provides a good illustration: just as φ_p is essentially the same as $(\frac{d}{p})$, so is φ_{-1} essentially the same as the sign $\operatorname{sign}(d)$ of d.

Quadratic reciprocity

To explain Artin's reciprocity law, we return to the quadratic ring $\mathbf{Q}[\sqrt{d}]$. In that case knowing φ_p is tantamount to knowing $(\frac{d}{p})$, and Artin's reciprocity law is just a disguised version of the *quadratic reciprocity law*. The latter states that for any two distinct odd prime numbers p and q one has

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4, \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

At first sight, this is hardly believable: $(\frac{q}{p})$ is defined by a congruence modulo p, and $(\frac{p}{q})$ by a congruence modulo q; what can these have to do with each other, when p and q are coprime? Nevertheless, the law is a theorem: it is the *theorema fundamentale* from Gauss's *Disquisitiones arithmeticae* (1801). Gauss also proved the *supplementary laws*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv -1 \bmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8, \\ -1 & \text{if } p \equiv \pm 3 \bmod 8, \end{cases}$$

the first of which is in fact immediate from the definition of $(\frac{d}{p})$.

For our purposes it is convenient to use a different formulation of the quadratic reciprocity law. It goes back to Euler, who empirically discovered the law in the 1740's but was unable to prove it; we refer to the books by Weil [17] and Lemmermeyer [13] for the historical details.

Euler's quadratic reciprocity law. *Let d be an integer, and let p and q be prime numbers not dividing $2d$. Then we have*

$$p \equiv q \bmod 4d \implies \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right),$$

$$p \equiv -q \bmod 4d \implies \left(\frac{d}{p}\right) = sign(d) \cdot \left(\frac{d}{q}\right).$$

To derive this from Gauss's results, one first notes that $(\frac{d}{p})$ is clearly periodic in d with period p, when p is fixed. Thus, if we can put the symbol "upside down"—as Gauss's fundamental theorem allows us to do, when d is an odd prime—then one may expect that $(\frac{d}{p})$ is also a periodic function of p when d is fixed. In this way one can deduce Euler's quadratic reciprocity law from Gauss's version, at least when d is an odd prime number. The cases $d = -1$ and $d = 2$ are immediately clear from the supplementary laws, and the case of general d is now obtained from the rule $(\frac{d_1}{p})(\frac{d_2}{p}) = (\frac{d_1 d_2}{p})$.

Conversely, one can use Euler's formulation to deduce Gauss's version, simply by choosing $d = (q \pm p)/4$, the sign being such that d is an integer (see [8, Chap. III, Sec. 5]); and the supplementary laws are even easier. Thus, Euler's and Gauss's quadratic reciprocity laws carry substantially the same information.

Not only did Euler observe that the value of the quadratic symbol $(\frac{d}{p})$ depends only on p mod $4d$, he also noticed that $(\frac{d}{p})$ exhibits multiplicative properties "as a function of p". For example, if p, q, r are primes satisfying $p \equiv qr \bmod 4d$, then we have $(\frac{d}{p}) = (\frac{d}{q})(\frac{d}{r})$. Formulated in modern language, this leads to a special case of Artin reciprocity. Denote, for a non-zero integer m, by $(\mathbf{Z}/m\mathbf{Z})^*$ the multiplicative group of invertible elements of the ring $\mathbf{Z}/m\mathbf{Z}$. Let d again be any non-zero integer.

Artin's quadratic reciprocity law. *There exists a group homomorphism*

$$(\mathbf{Z}/4d\mathbf{Z})^* \longrightarrow \{\pm 1\}$$

with

$$(p \bmod 4d) \longmapsto \left(\frac{d}{p}\right)$$

for any prime p not dividing $4d$.

The law implies, for example, that for prime numbers $p_1, p_2, \ldots, p_t$ satisfying $p_1 p_2 \cdots p_t \equiv 1 \bmod 4d$ one has $(\frac{d}{p_1}) \cdot (\frac{d}{p_2}) \cdot \ldots \cdot (\frac{d}{p_t}) = 1$.

To prove this multiplicative property, one first defines $(\frac{d}{n})$ for *any* positive integer n that is coprime to $2d$, by starting from the prime case and using the rule $(\frac{d}{n_1 n_2}) = (\frac{d}{n_1}) \cdot (\frac{d}{n_2})$. Next one shows, again starting from the prime case, that Gauss's results remain valid in this generality whenever they make sense, and one concludes that Euler's version carries over too. The symbol is now *by definition* multiplicative in its lower argument, so it is automatic that one obtains a group homomorphism. It maps $(-1 \bmod 4d)$ to $\mathrm{sign}(d)$.

Artin reciprocity over Q

If we wish to generalize Artin's quadratic reciprocity law to the situation of Theorem 2, it is natural to guess that $4d$ is to be replaced by $\Delta(f)$, and $(\frac{d}{p})$ by φ_p. This guess is correct. Let the polynomial f, the ring $\mathbf{Q}[\alpha]$, the abelian group G, and the Artin symbols φ_p for p not dividing $\Delta(f)$ be as in Theorem 2.

Artin reciprocity over Q. *There exists a group homomorphism*

$$(\mathbf{Z}/\Delta(f)\mathbf{Z})^* \longrightarrow G$$

with

$$(p \bmod \Delta(f)) \longmapsto \varphi_p$$

for any prime number p not dividing $\Delta(f)$. It is surjective if and only if f is irreducible.

The map is called the *Artin map* or the *reciprocity map*. It sends, appropriately enough, $(-1 \bmod \Delta(f))$ to φ_{-1}. The assertion about its surjectivity is obtained from Result 2.

Artin's reciprocity law does not exhibit any symmetry that would justify the term "reciprocity". The name derives from the fact that it extends the quadratic reciprocity law, and that its generalization to number fields extends similar "higher power" reciprocity laws. Still, something can be saved: from Result 1 we know that φ_p determines the splitting behavior of the polynomial f modulo p, so Artin reciprocity yields a relation between $(f \bmod p)$ and $(p \bmod \Delta(f))$ (cf. [18]).

In our cubic example $f = X^3 + X^2 - 2X - 1$ we have $\Delta(f) = 49$, and G is of order 3. Thus, the reciprocity law implies that the table of Artin symbols that we gave for f is periodic with period dividing 49. Better still: the period can be no more than 7, since it is not hard to show that any group homomorphism from $(\mathbf{Z}/49\mathbf{Z})^*$ to a group of order 3 factors through the natural map $(\mathbf{Z}/49\mathbf{Z})^* \to (\mathbf{Z}/7\mathbf{Z})^*$. This is what the reader may have perceived: one has $\varphi_p = 1$, σ, or τ according as $p \equiv \pm 1$, ± 2, or ± 3 mod 7. It is a general phenomenon for higher degree extensions that the number $\Delta(f)$ in our formulation of the reciprocity law can be replaced by a fairly small divisor.

Cyclotomic extensions

Artin's reciprocity law over $\mathbf{Q}$ generalizes the quadratic reciprocity law, and it may be thought that its mysteries lie deeper. Quite the opposite is true: the added generality is the first step on the way to a natural proof. It depends on the study of *cyclotomic extensions*.

Let m be a positive integer, and define the *m-th cyclotomic polynomial* $\Phi_m \in \mathbf{Z}[X]$ to be the product of those irreducible factors of $X^m - 1$ in $\mathbf{Z}[X]$ with leading coefficient 1 that do not divide $X^d - 1$ for any divisor $d < m$ of m. One readily proves the identity

$$\prod_d \Phi_d = X^m - 1,$$

where the product ranges over all divisors d of m. From this one can derive that the degree of Φ_m equals $\varphi(m) =$

$\#(\mathbf{Z}/m\mathbf{Z})^*$. The discriminant $\Delta(\Phi_m)$ divides the discriminant of $\Delta(X^m-1)$, which equals $\pm m^m$. For example, the discriminant of $\Phi_8 = (X^8-1)/(X^4-1) = X^4+1$, which equals 2^8, divides $\Delta(X^8-1) = -2^{24}$.

Denoting by ζ_m a "formal" zero of Φ_m, we obtain a ring $\mathbf{Q}[\zeta_m]$ that has vector space dimension $\varphi(m)$ over $\mathbf{Q}$. We have $\zeta_m^m = 1$, but $\zeta_m^d \neq 1$ when $d < m$ divides m, so the multiplicative order of ζ_m equals m. In the polynomial ring over $\mathbf{Q}[\zeta_m]$, the identity

$$\Phi_m = \prod_{a \in (\mathbf{Z}/m\mathbf{Z})^*} (X - \zeta_m^a)$$

is valid. One deduces that for each $a \in (\mathbf{Z}/m\mathbf{Z})^*$, the ring $\mathbf{Q}[\zeta_m]$ has an automorphism ϕ_a that maps ζ_m to ζ_m^a, and that $G = \{\phi_a : a \in (\mathbf{Z}/m\mathbf{Z})^*\}$ is a group isomorphic to $(\mathbf{Z}/m\mathbf{Z})^*$; in particular, it is abelian. This places us in the situation of Theorem 2, with $f = \Phi_m$ and $\alpha = \zeta_m$. Applying the theorem, we find $\varphi_p = \phi_p$ for all primes p not dividing m: all q_i in the theorem vanish! Artin's reciprocity law is now almost a tautology: if we identify G with $(\mathbf{Z}/m\mathbf{Z})^*$, the Artin map

$$(\mathbf{Z}/\Delta(\Phi_m)\mathbf{Z})^* \longrightarrow (\mathbf{Z}/m\mathbf{Z})^*$$

is simply the map sending $(a \bmod \Delta(\Phi_m))$ to $(a \bmod m)$ whenever a is coprime to m. This map is clearly surjective, so we recover the well-known fact that Φ_m is irreducible in $\mathbf{Z}[X]$. Thus, our cyclotomic ring is actually a field.

We conclude that for cyclotomic extensions, Artin's reciprocity law can be proved by means of a plain verification. One can now attempt to prove Artin's reciprocity law in other cases by reduction to the cyclotomic case. For example, the supplementary law that gives the value of $(\frac{2}{p})$ is a consequence of the fact that $\zeta_8 + \zeta_8^{-1}$ is a square root of 2. Namely, one has

$$\varphi_p(\sqrt{2}) = \varphi_p(\zeta_8 + \zeta_8^{-1}) \equiv (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \bmod p;$$

for $p \equiv \pm 1 \bmod 8$, this equals

$$\zeta_8 + \zeta_8^{-1} = \sqrt{2},$$

and for $p \equiv \pm 3 \bmod 8$ it is

$$\zeta_8^3 + \zeta_8^{-3} = \zeta_8^4 \cdot (\zeta_8 + \zeta_8^{-1}) = -\sqrt{2}.$$

This confirms that in the two respective cases one has $(\frac{2}{p}) = 1$ and $(\frac{2}{p}) = -1$.

The reader may enjoy checking that our example $f = X^3 + X^2 - 2X - 1$ can also be reduced to the cyclotomic case: if ζ_7 is a zero of $\Phi_7 = (X^7-1)/(X-1) = \sum_{i=0}^{6} X^i$, then $\alpha = \zeta_7 + \zeta_7^{-1}$ is a zero of f, and one finds

$$\varphi_p(\alpha) = \zeta_7^p + \zeta_7^{-p} = \begin{cases} \zeta_7 + \zeta_7^{-1} = \alpha & \text{for } p \equiv \pm 1 \bmod 7, \\ \zeta_7^2 + \zeta_7^{-2} = \alpha^2 - 2 = \sigma(\alpha) & \text{for } p \equiv \pm 2 \bmod 7, \\ \zeta_7^3 + \zeta_7^{-3} = \alpha^3 - 3\alpha = \tau(\alpha) & \text{for } p \equiv \pm 3 \bmod 7. \end{cases}$$

This proves our observation on the pattern underlying the table of Artin symbols.

The theorem of Kronecker-Weber (1887) implies that the reduction to cyclotomic extensions will always be successful. This theorem, which depends on a fair amount of algebraic number theory, asserts that every Galois extension of $\mathbf{Q}$ with an abelian Galois group can be embedded in a cyclotomic extension (see [14, Chap. 6]). That takes care of the case in which f is irreducible, from which the general case follows easily. In particular, to prove the quadratic reciprocity law it suffices to express square roots of integers in terms of roots of unity, as we just did with $\sqrt{2}$. Such expressions form the basis of one of Gauss's many proofs for his fundamental theorem.

Algebraic number theory

A *number field* is an extension field K of $\mathbf{Q}$ that is of finite dimension as a vector space over $\mathbf{Q}$. We saw already many of them in the preceding sections, but now their role will be different: they will replace $\mathbf{Q}$ as the *base field* in Artin's reciprocity law. Formulating the latter requires the analogue for K of several concepts that are taken for granted in the case of $\mathbf{Q}$, such as the subring $\mathbf{Z}$ of $\mathbf{Q}$ and the notion of a prime number. The facts that we need are easy enough to state, but their proofs take up most of a first course in algebraic number theory.

An element of a number field K is called an *algebraic integer* if it is a zero of a polynomial in $\mathbf{Z}[X]$ with leading coefficient 1. The set $\mathbf{Z}_K$ of algebraic integers in K is a subring of K that has K as its field of fractions. For $K = \mathbf{Q}$ it is $\mathbf{Z}$.

The theorem of unique prime factorization is not generally valid in $\mathbf{Z}_K$, and ideals have been invented in order to remedy this regrettable situation. We recall that a subset of a ring R is called an *ideal* if it is the kernel of a ring homomorphism that is defined on R or, equivalently, if it is an additive subgroup of R that is closed under multiplication by elements of R. An ideal is *prime* if it is the kernel of a ring homomorphism from R to some *field*. The *product* $\mathfrak{ab}$ of two ideals $\mathfrak{a}$, $\mathfrak{b}$ is the ideal consisting of all sums $\mu_1\nu_1 + \mu_2\nu_2 + \cdots + \mu_t\nu_t$ with $\mu_i \in \mathfrak{a}$, $\nu_i \in \mathfrak{b}$. For example, the ideals of the ring $\mathbf{Z}$ are the subsets of the form $m\mathbf{Z}$, where m is a non-negative integer; $m\mathbf{Z}$ is a prime ideal if and only if m is a prime number or 0, and multiplying two ideals comes down to multiplying the corresponding m's.

In the ring $\mathbf{Z}_K$, the theorem of unique prime *ideal* factorization is valid: each non-zero ideal $\mathfrak{a}$ can be written as a product $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t$ of non-zero prime ideals $\mathfrak{p}_i$, and this representation is unique up to order. Several basic relations between ideals can be read from their prime ideal factorizations. For example, one ideal contains another if and only if it "divides" it in an obvious sense; and two non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ have no prime ideal in common in their factorizations if and only if they are "coprime" in the sense that $\mu + \nu = 1$ for some $\mu \in \mathfrak{a}$, $\nu \in \mathfrak{b}$. One recognizes familiar properties of positive integers.

Instead of "non-zero prime ideal of $\mathbf{Z}_K$", we shall also say "prime of K". More correctly, we should say "*finite* prime of K", since a full appreciation of the arithmetic of number fields requires the consideration of so-called "infinite primes" as well. For example, $K = \mathbf{Q}$ has just one infinite prime, and it gave rise to the "exotic" Artin symbol φ_{-1}. For our purposes we can afford to disregard infinite primes for general K, at the expense of one more definition: an element $\nu \in K$ is called *totally positive* if each field embedding $K \to \mathbf{R}$ maps ν to a positive real number and (in case there are no such embeddings) $\nu \neq 0$; notation: $\nu \gg 0$. For example, in the case $K = \mathbf{Q}$ one has $\nu \gg 0$ if and only if $\nu > 0$; and if K contains a square root of a negative integer, then one has $-1 \gg 0$.

Primes in a quadratic field

We illustrate the results of the preceding section with the field $K = \mathbf{Q}[\sqrt{-7}]$. The element $\omega = (1 + \sqrt{-7})/2$ of K belongs to $\mathbf{Z}_K$, since it is a zero of the polynomial $X^2 - X + 2$. One has in fact $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z} \cdot \omega$. The unique non-trivial automorphism of K is denoted by an overhead bar; thus, one has $\bar{\omega} = 1 - \omega$.

Finding a ring homomorphism from $\mathbf{Z}_K$ to another ring is equivalent to finding a zero of $X^2 - X + 2$ in that ring. For example, the element $-2 \in \mathbf{Z}/8\mathbf{Z}$ satisfies $(-2)^2 - (-2) + 2 = 8 = 0$, so there is a ring homomorphism

$$\begin{aligned} \mathbf{Z}_K &\longrightarrow \mathbf{Z}/8\mathbf{Z}, \\ a + b \cdot \omega &\longmapsto (a - 2b \bmod 8). \end{aligned}$$

Since this map is "defined" by putting $8 = 0$ and $\omega = -2$, its kernel $\mathfrak{a}$ is generated by 8 and $\omega + 2$. The easily verified equality $8 = (\omega + 2)(\bar{\omega} + 2) \in (\omega + 2)\mathbf{Z}_K$ shows that a single generator suffices: $\mathfrak{a} = (\omega + 2)\mathbf{Z}_K$.

Standard computational techniques from algebraic number theory show that in our example *every* ideal of $\mathbf{Z}_K$ has the form $\mu\mathbf{Z}_K$, with $\mu \in \mathbf{Z}_K$. One may think that this is an exceptional property of K; indeed, it implies unique factorization for elements rather than just for ideals, which is known to fail for infinitely many (non-isomorphic) number fields. However, recent computational results and heuristic arguments [6] suggest that this property is actually very common, especially among number fields of "high" dimension over $\mathbf{Q}$. This feeling is not supported by any known theorem.

For $K = \mathbf{Q}[\sqrt{-7}]$, it is also true that the generator $\mu \in \mathbf{Z}_K$ of an ideal $\mu\mathbf{Z}_K$ is unique up to multiplication by ± 1. Just as for $\mathfrak{a} = (\omega + 2)\mathbf{Z}[\omega]$ above, the ring $\mathbf{Z}[\omega]/\mu\mathbf{Z}[\omega]$ is finite of cardinality $\mu\bar{\mu}$ for every $\mu \neq 0$.

Let us now look into the *primes* of K. Finding these comes down to finding zeroes of $X^2 - X + 2$ in *finite fields*. A central role is played by the finite fields of the form $\mathbf{F}_p$, for p prime. Over the field $\mathbf{F}_2$, one has $X^2 - X + 2 = X(X - 1)$, which gives rise to two ring homomorphisms $\mathbf{Z}_K \to \mathbf{F}_2$: one that maps ω to $0 \in \mathbf{F}_2$, and one that maps ω to $1 \in \mathbf{F}_2$. Their kernels are two prime ideals of index 2 of $\mathbf{Z}_K$, with respective generators ω and $\bar{\omega}$. Note that we have $\omega\bar{\omega} = 2$. The identity $\omega + 2 = -\omega^3$ shows that the ideal $\mathfrak{a}$ considered above factors as the cube of the prime $\omega\mathbf{Z}_K$.

Similarly, let p be an odd prime number with $(\frac{-7}{p}) = 1$; by the quadratic reciprocity law, the latter condition is equivalent to $(\frac{p}{7}) = 1$, i.e., to $p \equiv 1, 2$, or $4 \bmod 7$. Then -7 has a square root in $\mathbf{F}_p$, and since $X^2 - X + 2$ has discriminant -7, it has two different zeroes in $\mathbf{F}_p$. As before, these give rise to two prime ideals $\pi\mathbf{Z}_K$ and $\bar{\pi}\mathbf{Z}_K$ of index $\pi\bar{\pi} = p$ in $\mathbf{Z}_K$.

Modulo 7, the polynomial $X^2 - X + 2$ has a double zero at 4, which leads to the prime ideal $\sqrt{-7}\mathbf{Z}_K$ of index 7. Generally, finding zeroes of $X^2 - X + 2$ in finite fields containing $\mathbf{F}_p$ amounts to factoring $X^2 - X + 2$ in $\mathbf{F}_p[X]$, which explains the relevance of Result 1 for the purpose of finding prime ideals. In fact, the

present considerations could have been made to depend on the Artin symbol for the extension $K = \mathbf{Q}[\omega]$ of $\mathbf{Q}$. Let, for example, p be one of the remaining prime numbers; so $p \equiv 3, 5$, or $6 \bmod 7$. Then the Artin symbol equals -1, the polynomial $X^2 - X + 2$ is irreducible in $\mathbf{F}_p[X]$, and $p\mathbf{Z}_K$ is a prime ideal for which $\mathbf{Z}_K/p\mathbf{Z}_K$ is a finite field of cardinality p^2. These prime ideals are of lesser importance for us. They complete the enumeration of primes of K.

Discovering the laws of arithmetic in a specific number field, as we just did for $\mathbf{Q}[\sqrt{-7}]$, is not only an agreeable enterprise in its own right, it also has applications to the solution of equations in ordinary integers. The following theorem provides a classical illustration.

Theorem. *Let p be an odd prime number congruent to* 1, 2, *or* 4 mod 7. *Then p can be written as*

$$p = x^2 + 7y^2$$

for certain integers x and y; moreover, x and y are uniquely determined up to sign.

To prove this, let $p = \pi\bar{\pi}$ as above, with $\pi \in \mathbf{Z}_K$. Writing $\pi = a + b\omega$, with $a, b \in \mathbf{Z}$, one obtains

$$p = \pi\bar{\pi} = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab + 2b^2.$$

Clearly, $a(a + b)$ is odd, so a is odd and b is even; writing $b = 2y$ and $a + y = x$ we obtain the desired representation. Uniqueness is a consequence of unique prime ideal factorization.

Number theorists of all persuasions have been fascinated by prime numbers of the form $2^l - 1$ ever since Euclid (∼300 B.C.) used them for the construction of *perfect numbers*. In modern times they are named after Marin Mersenne (1588–1648). The *Mersenne number* $M_l = 2^l - 1$ can be prime only if l is itself prime; M_l is indeed prime for $l = 2, 3, 5, 7, 13, 17, 19, 31$, and conjecturally infinitely many other values of l, whereas it is composite for $l = 11, 23, 29, 37, 41, 43, 47, 53$, and conjecturally infinitely many other prime values of l. One readily shows that a Mersenne prime M_l is 1, 2, or 4 mod 7 if and only if $l \equiv 1 \bmod 3$, in which case one actually has $M_l \equiv 1 \bmod 7$. Here are the first few such Mersenne primes, as well as their representations as $x^2 + 7y^2$:

$$\begin{aligned} M_7 &= 127 = 8^2 + 7 \cdot 3^2, \\ M_{13} &= 8191 = 48^2 + 7 \cdot 29^2, \\ M_{19} &= 524287 = 720^2 + 7 \cdot 29^2, \\ M_{31} &= 2147483647 = 43968^2 + 7 \cdot 5533^2, \\ M_{61} &= 2305843009213693951 = 910810592^2 + 7 \cdot 459233379^2. \end{aligned}$$

This table was made by Franz Lemmermeyer. He observed that in each case x is divisible by 8, a phenomenon that persisted when larger Mersenne primes were tried. A small computation modulo 8 shows that x is necessarily divisible by 4. Modulo higher powers of 2 one finds that y is $\pm 3 \bmod 8$, but one learns nothing new about x. Maybe the divisibility by 8 is just an accident?

Abelian extensions

In order to formulate the analogue of Theorem 2 over an arbitrary number field K, we need to extend the notion of Frobenius map. For a prime $\mathfrak{p}$ of K, we write $k(\mathfrak{p}) = \mathbf{Z}_K/\mathfrak{p}$; this is a finite field, and its cardinality is called the *norm* $\mathfrak{N}\mathfrak{p}$ of $\mathfrak{p}$. Instead of rings with "$p = 0$" for some prime number p, we consider rings R that come equipped with a ring homomorphism $k(\mathfrak{p}) \to R$ for some prime $\mathfrak{p}$ of K. The *Frobenius map* F (relative to $\mathfrak{p}$) of such a ring is the map $R \to R$ defined by $F(x) = x^{\mathfrak{N}\mathfrak{p}}$. It is a ring homomorphism. Galois proved in 1830 that the Frobenius map of the finite field $k(\mathfrak{p})$ itself is the identity map. This generalizes Fermat's little theorem.

Next we "lift" Frobenius maps to Artin symbols. To give a succinct description of the situation in which this can be done, we borrow a definition from *Galois theory for rings*. Let L be a ring that contains K, such that the dimension n of L as a vector space over K is finite. We assume that we are given an abelian group G of n automorphisms of L that are the identity on K, such that for some K-basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ of L the matrix $A = \big(\sigma\varepsilon_i\big)_{1 \le i \le n,\, \sigma \in G}$ is invertible as a matrix over L. In this situation one says that L is an abelian (ring) extension of K with group G. The abelian ring extensions of $K = \mathbf{Q}$ are exactly the rings $\mathbf{Q}[\alpha]$ encountered in Theorem 2; but the present definition avoids reference to a specific defining polynomial f.

With L and G as above, one defines the subring $\mathbf{Z}_L$ of L in the same way as we did for $L = K$ in the previous section, and one defines the discriminant $\Delta(L/K)$ to be the $\mathbf{Z}_K$-ideal generated by the numbers $(\det A)^2$, as A ranges over all matrices as above that are obtained from elements $\varepsilon_1, \ldots, \varepsilon_n$ of $\mathbf{Z}_L$; all these numbers lie in $\mathbf{Z}_K$. In the case $K = \mathbf{Q}$, this discriminant divides the discriminant $\Delta(f)$ considered earlier. We can now state the analogue of Theorem 2.

Theorem 3. *Let K be a number field, and let L be an abelian extension of K with group G. Then for every prime $\mathfrak{p}$ of K that does not divide $\Delta(L/K)$, there is a unique element $\varphi_\mathfrak{p} \in G$ with the property that the automorphism of $\mathbf{Z}_L/\mathfrak{p}\mathbf{Z}_L$ induced by $\varphi_\mathfrak{p}$ is the Frobenius map of $\mathbf{Z}_L/\mathfrak{p}\mathbf{Z}_L$ relative to $\mathfrak{p}$.*

Here we write $\mathfrak{p}\mathbf{Z}_L$ for the $\mathbf{Z}_L$-ideal generated by $\mathfrak{p}$; the inclusion map $\mathbf{Z}_K \to \mathbf{Z}_L$ induces a ring homomorphism $k(\mathfrak{p}) \to \mathbf{Z}_L/\mathfrak{p}\mathbf{Z}_L$, so that the latter ring has indeed a well-defined Frobenius map relative to $\mathfrak{p}$. The element $\varphi_\mathfrak{p} \in G$ is again called the *Artin symbol* of $\mathfrak{p}$. What we said about the proof of Theorem 2 applies here as well.

To give an example, we return to $K = \mathbf{Q}[\sqrt{-7}] = \mathbf{Q}[\omega]$, with $\omega^2 - \omega + 2 = 0$, and we take $L = K[\beta]$, where β is a zero of $X^2 - \omega X - 1$. Since the discriminant $\omega^2 + 4 = \omega + 2$ of the latter polynomial is non-zero, and L has dimension 2 over K, it is automatic that L is abelian over K with a group G of order 2; the non-identity element ρ of G satisfies $\rho(\beta) = \omega - \beta = -1/\beta$. One can show that $\mathbf{Z}_L$ equals $\mathbf{Z}_K + \mathbf{Z}_K \cdot \beta$, and that this in turn implies that $\Delta(L/K)$ is the $\mathbf{Z}_K$-ideal generated by the polynomial discriminant $\omega + 2$; it is the ideal $\mathfrak{a} = (\omega\mathbf{Z}_K)^3$ from the previous section.

Let us compute $\varphi_\mathfrak{p}$ for the prime $\mathfrak{p} = \sqrt{-7}\mathbf{Z}_K$ of norm 7 in this example. In the field $k(\mathfrak{p}) = \mathbf{F}_7$ we have $2\omega - 1 = \sqrt{-7} = 0$, and therefore $\omega = 4$. The ring $\mathbf{Z}_L/\mathfrak{p}\mathbf{Z}_L$ is the quadratic extension $\mathbf{F}_7[\beta]$ of $\mathbf{F}_7$ defined by $\beta^2 = \omega\beta + 1 = 4\beta + 1$. An easy computation shows that in that ring one has $\beta^{\mathfrak{N}\mathfrak{p}} = \beta^7 = 4 - \beta$. This is the same as the image of $\rho(\beta) = \omega - \beta$ in $\mathbf{Z}_L/\mathfrak{p}\mathbf{Z}_L$, so we have $\varphi_\mathfrak{p} = \rho$. The computationally oriented reader is invited to check in a similar way that each of the two primes $(8 \pm 3\sqrt{-7})\mathbf{Z}_K$ of norm $M_7 = 127$ has Artin symbol 1.

Artin's reciprocity law

Artin's reciprocity law in its general formulation is one of the main results of *class field theory*. As we remarked in the introduction, there is no royal road to this subject, but the most convenient one surely starts from the observation that the theorems of class field theory are, in their formulation, the simplest ones that have a chance of being true; indeed, the simplest ones that are *meaningful*. Artin's reciprocity law provides an apt illustration.

Let us place ourselves in the situation of Theorem 3, and ask what a generalization of Artin's reciprocity law to K might look like. Superficially, this seems to be an easy question, since every ingredient of the law for $\mathbf{Q}$ has a meaningful analogue over K. In particular, the natural replacement for the group $(\mathbf{Z}/m\mathbf{Z})^*$, which we defined for any non-zero integer m, is the group of invertible elements $(\mathbf{Z}_K/\mathfrak{m})^*$ of the finite ring $\mathbf{Z}_K/\mathfrak{m}$, for a non-zero $\mathbf{Z}_K$-ideal $\mathfrak{m}$. However, closer inspection reveals a difficulty: if $\mathfrak{p}$ is a prime of K coprime to $\Delta(L/K)$, there is no way to give a meaningful interpretation to "$\mathfrak{p}$ mod $\Delta(L/K)$" as an element of $(\mathbf{Z}_K/\Delta(L/K))^*$.

This is the only problem we need to resolve: defining, for a non-zero ideal $\mathfrak{m}$ of $\mathbf{Z}_K$, a suitable "multiplicative" group "modulo $\mathfrak{m}$" that contains an element "$\mathfrak{p}$ mod $\mathfrak{m}$" for each $\mathfrak{p}$ coprime to $\mathfrak{m}$, and that generalizes $(\mathbf{Z}/m\mathbf{Z})^*$. The desired group is called the *ray class group modulo* $\mathfrak{m}$, and we shall denote it by $\mathrm{Cl}_\mathfrak{m}$. Anybody who has assimilated its definition is ready to appreciate class field theory.

Here is a description of $\mathrm{Cl}_\mathfrak{m}$ by means of generators and relations: one generator $[\mathfrak{p}]$ for each prime $\mathfrak{p}$ of $\mathbf{Z}_K$ coprime to $\mathfrak{m}$, and one relation $[\mathfrak{p}_1]\cdot[\mathfrak{p}_2]\cdot\ldots\cdot[\mathfrak{p}_t]=1$ for every sequence $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ of prime ideals for which there exists $\nu\in\mathbf{Z}_K$ satisfying

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t=\nu\mathbf{Z}_K,\qquad \nu\equiv 1 \bmod \mathfrak{m},\qquad \nu\gg 0.$$

One can show that this definition has all the desired properties, and that $\mathrm{Cl}_\mathfrak{m}$ is a finite abelian group. Using unique prime ideal factorization, one can reformulate the definition by saying that $\mathrm{Cl}_\mathfrak{m}$ is the multiplicative group of equivalence classes of non-zero ideals $\mathfrak{a}$ of $\mathbf{Z}_K$ that are coprime to $\mathfrak{m}$, where $\mathfrak{a}_1$ belongs to the same class as $\mathfrak{a}_2$ if and only if there exist $\nu_1, \nu_2\in\mathbf{Z}_K$ with

$$\nu_1\mathfrak{a}_1=\nu_2\mathfrak{a}_2,\qquad \nu_1\equiv\nu_2\equiv 1 \bmod \mathfrak{m},\qquad \nu_1\gg 0,\qquad \nu_2\gg 0.$$

The reader who wishes to ponder this definition may show that it does generalize $(\mathbf{Z}/m\mathbf{Z})^*$, which it would not without the total positivity conditions. More generally, there is a group homomorphism from our "first guess" $(\mathbf{Z}_K/\mathfrak{m})^*$ to $\mathrm{Cl}_\mathfrak{m}$ that sends $(\upsilon \bmod \mathfrak{m})$ to the class of $\upsilon\mathbf{Z}_K$ whenever $\upsilon\gg 0$; and although in general it is neither injective nor surjective, it is both for $K=\mathbf{Q}$.

We have reached the high point of the journey. Let the situation be as in Theorem 3.

Artin's reciprocity law. *There is a group homomorphism*

$$\mathrm{Cl}_{\Delta(L/K)}\longrightarrow G$$

with

$$[\mathfrak{p}]\ \longmapsto\ \varphi_\mathfrak{p}$$

for every prime $\mathfrak{p}$ *of* K *coprime to* $\Delta(L/K)$. *It is surjective if and only if* L *is a field.*

We shall again call this map the *Artin map*. By definition of $\mathrm{Cl}_{\Delta(L/K)}$, the theorem asserts that we have

$$\varphi_{\mathfrak{p}_1}\cdot\varphi_{\mathfrak{p}_2}\cdot\ldots\cdot\varphi_{\mathfrak{p}_t}=1$$

whenever $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ satisfy $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t=\nu\mathbf{Z}_K$ for some $\nu\equiv 1 \bmod \Delta(L/K)$ with $\nu\gg 0$. This is just as unreasonable as the quadratic reciprocity law: the Artin symbols $\varphi_\mathfrak{p}$ are defined locally at the prime ideals $\mathfrak{p}$, and appear to be completely independent for different primes; how is it that they can "see" a global relationship satisfied by these primes?

In the case $K=\mathbf{Q}$ the Kronecker-Weber theorem may be felt to provide an adequate explanation of "why" the reciprocity law is true. For $K\neq\mathbf{Q}$, the immediate generalization of the Kronecker-Weber theorem is false. Finding a usable substitute is the content of Hilbert's twelfth problem, which is still outstanding.

When Artin formulated his reciprocity law in 1923, he could do no more than postulate its validity. It was only four years later that he was able to provide a proof, borrowing the essential idea from the Russian mathematician Nikolai Grigor'evich Chebotarëv. He was just in time, since Chebotarëv was in the process of constructing a proof himself [15]. Curiously, Chebotarëv's idea *also* reduces the proof to the cyclotomic case, but the reduction is not nearly as direct as it is over $\mathbf{Q}$.

Mersenne primes

Let us examine what Artin reciprocity comes down to in the example

$$\begin{aligned} K &= \mathbf{Q}[\sqrt{-7}]=\mathbf{Q}[\omega], & \omega^2-\omega+2 &= 0,\\ L &= K[\beta], & \beta^2-\omega\beta-1 &= 0 \end{aligned}$$

considered earlier. We know already that $\Delta(L/K)=\mathfrak{a}$ is the kernel of the map $\mathbf{Z}_K\to\mathbf{Z}/8\mathbf{Z}$ sending ω to -2, and that it is the cube of the prime $\omega\mathbf{Z}_K$ of norm 2.

First we need to compute $\mathrm{Cl}_\mathfrak{a}$. The reader who did give some thought to ray class groups will have no trouble verifying that the map $(\mathbf{Z}/8\mathbf{Z})^*\cong(\mathbf{Z}_K/\mathfrak{a})^*\to\mathrm{Cl}_\mathfrak{a}$ defined in the previous section is surjective, and that its kernel is $\{\pm 1\}$. Hence we may identify $\mathrm{Cl}_\mathfrak{a}$ with the group $(\mathbf{Z}/8\mathbf{Z})^*/\{\pm 1\}$ of order 2.

Consider next the Artin map $\mathrm{Cl}_\mathfrak{a}\to G=\{1,\rho\}$. It can't be the trivial map, since the Artin symbol of the prime $\sqrt{-7}\mathbf{Z}_K$ is ρ; hence it is an isomorphism, and, by the theorem, L is a field. In other words, the discriminant $\omega+2=-\omega^3$ of the polynomial defining L is not a square in K, which can also be seen directly. We have $L=K[\sqrt{-\omega}]$.

Unravelling the various maps, we arrive at the following simple recipe for computing Artin symbols in L:

> *if* $\mathfrak{p}=\pi\mathbf{Z}_K$ *is a prime of* K *different from* $\omega\mathbf{Z}_K$, *then* $\varphi_\mathfrak{p}$ *equals* 1 *or* ρ *according as* π *maps to* ± 1 *or to* ± 3 *under the map* $\mathbf{Z}_K\to\mathbf{Z}/8\mathbf{Z}$ *that sends* ω *to* -2.

For example, $\sqrt{-7}=2\omega-1$ maps to 3, confirming what we know about its Artin symbol. The numbers $8\pm 3\sqrt{-7}$ map to $\pm 3\cdot 3=\pm 1$, so even the reader who is *not* computationally oriented can now conclude that both primes of norm 127 have Artin symbol equal to 1.

More generally, consider any Mersenne prime M_l with $l\equiv 1 \bmod 3$, and write $M_l=x^2+7y^2$, with $x, y\in\mathbf{Z}$. Then $x+y\sqrt{-7}$ generates a prime of norm M_l of K. Our recipe tells us that its Artin symbol equals 1 if $x+3y$ is $\pm 1 \bmod 8$, and ρ otherwise.

Since we know $x \equiv 0 \bmod 4$ and $y \equiv \pm 3 \bmod 8$, the Artin symbol is 1 if and only if x is divisible by 8. In other words, the property of Mersenne primes observed by Lemmermeyer is equivalent to the assertion that any prime of $K = \mathbf{Q}[\sqrt{-7}]$ of norm M_l has trivial Artin symbol in the quadratic extension $L = K[\sqrt{-\omega}]$.

Surprisingly, we can use this reformulation to obtain a proof of Lemmermeyer's observation. Waving the magic wand of Galois theory we shall transform the base field $\mathbf{Q}[\sqrt{-7}]$ into $\mathbf{Q}[\sqrt{2}]$. Moving back and forth via the Artin symbol, we find that the alleged property of primes of norm M_l in the first field translates into a similar property of primes of norm M_l in the second field. As one may expect, the field $\mathbf{Q}[\sqrt{2}]$ has a natural affinity for the numbers $2^l - 1$, which leads to a rapid conclusion of the argument.

Theorem. *Let $M_l = 2^l - 1$ be a Mersenne prime with $l \equiv 1 \bmod 3$, and write $M_l = x^2 + 7y^2$ with $x, y \in \mathbf{Z}$. Then x is divisible by 8.*

The proof operates in the extension $N = K[\sqrt{-\omega}, \sqrt{-\bar{\omega}}]$ of K that is "composed" of the quadratic extension $L = K[\sqrt{-\omega}]$ and its conjugate $K[\sqrt{-\bar{\omega}}]$. The dimension of N over K is 4, a basis consisting of 1, $\sqrt{-\omega}$, $\sqrt{-\bar{\omega}}$, and $\sqrt{-\omega}\sqrt{-\bar{\omega}} = \sqrt{2}$. It suffices to prove the congruence

$$\xi^{M_l} \equiv \xi \bmod M_l \mathbf{Z}_N \qquad \text{for all } \xi \in \mathbf{Z}_N,$$

since it implies that the Artin symbols of both primes of norm M_l of K in the subextension L of N are trivial.

If an extension can be written, just like N, as the composition of a "twofold" quadratic extension of $\mathbf{Q}$ with its conjugate, then there is a *second* way to write it in that manner. This is a generality from Galois theory; it is due to the dihedral group of order 8 possessing an outer automorphism.

In plain terms, N contains $\sqrt{2}$, and may be viewed as an extension of dimension 4 of the field $E = \mathbf{Q}[\sqrt{2}]$. From the identity

$$(\sqrt{-\omega} \pm \sqrt{-\bar{\omega}})^2 = -(\omega + \bar{\omega}) \pm 2\sqrt{-\omega}\sqrt{-\bar{\omega}} = -1 \pm 2\sqrt{2}$$

one deduces that N is the composition of two conjugate quadratic extensions of E, namely those obtained by adjoining square roots of $-1 + 2\sqrt{2}$ and $-1 - 2\sqrt{2}$. (The product of those square roots is a square root of -7.) It follows that N is an *abelian* extension of E.

In the new base field E, we can explicitly factor M_l:

$$M_l = 2^l - 1 = \frac{\sqrt{2}^l - 1}{\sqrt{2} - 1} \cdot \frac{\sqrt{2}^l + 1}{\sqrt{2} + 1}.$$

Denote by ν_l and $\tilde{\nu}_l$ the two factors on the right. They belong to $\mathbf{Z}_E = \mathbf{Z} + \mathbf{Z} \cdot \sqrt{2}$, and they are conjugate in E. Just as in the case of K, they generate two primes of E of norm M_l. As ν_l and $\tilde{\nu}_l$ are coprime with product M_l, the congruence to be proved

is equivalent to

$$\xi^{M_l} \equiv \xi \bmod \nu_l \mathbf{Z}_N \quad \text{and}$$
$$\xi^{M_l} \equiv \xi \bmod \tilde{\nu}_l \mathbf{Z}_N \quad \text{for all } \xi \in \mathbf{Z}_N.$$

In other words: it suffices to show that the Artin symbols of $\nu_l \mathbf{Z}_E$ and $\tilde{\nu}_l \mathbf{Z}_E$ in the abelian extension N of E are both the identity.

We write $N = E[\gamma, \delta]$, where γ and δ are zeroes of the quadratic polynomials $X^2 - (1+\sqrt{2})X + 1$ and $X^2 - (1-\sqrt{2})X + 1$ of discriminants $-1+2\sqrt{2}$ and $-1-2\sqrt{2}$, respectively. An automorphism of N is the identity as soon as it is the identity on both $E[\gamma]$ and $E[\delta]$. Thus it is enough to show that the Artin symbols of $\nu_l \mathbf{Z}_E$ and $\tilde{\nu}_l \mathbf{Z}_E$ for the extensions $E[\gamma]$ and $E[\delta]$ are trivial. For this we invoke Artin reciprocity. The discriminant of each of these extensions divides $(-1+2\sqrt{2})(-1-2\sqrt{2})\mathbf{Z}_E = 7\mathbf{Z}_E$. From $l \equiv 1 \bmod 6$ and $\sqrt{2}^6 = 8 \equiv 1 \bmod 7$ one sees $\sqrt{2}^l \equiv \sqrt{2} \bmod 7$, so the generators ν_l and $\tilde{\nu}_l$ of our primes are both 1 mod $7\mathbf{Z}_E$. Also, they are readily seen to be totally positive. Hence, the Artin reciprocity law implies that their Artin symbols are trivial, as required.

The reader who dislikes the explicit manipulations in our argument will be reassured to learn that class field theory has theorems other than Artin's reciprocity law. Using these, one can establish the existence of the desired extensions without writing them down. This allows one, for example, to contemplate the possibility of formulating and proving a similar theorem that is not special to any particular number like 7.

In our proof, Artin's reciprocity law functioned as a bridge between ray class groups of two different number fields. It is actually possible to relate these ray class groups in a more elementary manner, by means of *genus theory*. There are also applications of Artin reciprocity to conjectured properties of Mersenne primes that do not appear to allow for similar simplifications [11].

Acknowledgments

The photographs of Emil Artin were kindly provided by Michael Artin.
The first author was supported by NSF under grant No. DMS 92-24205.

References

For a description of Artin's life and his personality Richard Brauer's obituary [4] is particularly recommended. An elaborate introduction into class field theory and its historical background is found in Cox's book [7]. The best modern account of the proofs is in Lang's textbook [12]. Indispensable for the would-be specialist is the Brighton proceedings volume edited by Cassels and Fröhlich [5].

1 E. Artin, *Collected papers*, Addison-Wesley, Reading, Mass., 1965.

2 E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ. Hamburg, **3** (1923/1924), no. 1 (1923), 89–108; [1], pp. 105–124.

3 E. Artin, *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Sem. Univ. Hamburg **5** (1926/1927), no. 4 (1927), 353–363; [1], pp. 131–141.

4 R. Brauer, *Emil Artin*, Bull. Amer. Math. Soc. **73** (1967), 27–43.

5 J. W. S. Cassels, A. Fröhlich, *Algebraic number theory*, Academic Press, London, 1967.

6 H. Cohen, H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, H. Jager (ed.), *Number theory, Noordwijkerhout 1983*, Lecture Notes in Math. **1068**, Springer-Verlag, Heidelberg, 1984, pp. 33–62.

7 D. A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, New York, 1989.

8 H. Davenport, *The higher arithmetic*, Hutchinson University Library, London, 1952.

9 G. Frei, *Die Briefe von E. Artin an H. Hasse (1923–1953)*, Université Laval, Québec, and Forschungsinstitut für Mathematik, ETH, Zürich, 1981.

10 F. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1896), 689–703; *Gesammelte Abhandlungen*, vol. II, Springer-Verlag, Berlin, 1968, pp. 719–733.

11 S. Y. Gebre-Egziabher, Ph. D. thesis, UC Berkeley (in preparation).

12 S. Lang, *Algebraic number theory*, second edition, Springer-Verlag, New York, 1994.

13 F. Lemmermeyer, *Reciprocity laws: their evolution from Euler to Artin*, Springer-Verlag, Berlin, to appear.

14 R. L. Long, *Algebraic number theory*, Marcel Dekker, New York, 1977.

15 P. Stevenhagen, H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer, **18** (1996), No. 2, pp. 26–37.

16 P. Tannery, C. Henry (eds), *Œuvres de Fermat*, vol. II, Gauthiers-Villars, Paris, 1894, p. 342; vol. III, ibid., 1896, p. 431; see also: R. Rashed, Ch. Houzel, G. Christol (intr., comm.), *Œuvres de Pierre Fermat I, La théorie des nombres*, Albert Blanchard, Paris, 1999, pp. 264, 286.

17 A. Weil, *Number theory, an approach through history*, Birkhäuser, Basel, 1983.

18 B. F. Wyman, *What is a reciprocity law?*, Amer. Math. Monthly **79** (1972), 571–586; correction, ibid. **80** (1973), 281.