Math 248A. Quadratic characters associated to quadratic fields

The aim of this handout is to describe the quadratic Dirichlet character naturally associated to a quadratic field, and to express it in terms of quadratic residue symbols.

1. Link with cyclotomic fields

Let K be a quadratic field with discriminant $D \in \mathbf{Z}$, so $D \equiv 0, 1 \bmod 4$ and $K = \mathbf{Q}(\sqrt{D}) = \mathbf{Q}(\sqrt{d})$ for a unique squarefree $d \neq 1$ with $D = 4d$ for even D (with $d \equiv 2, 3 \bmod 4$) and $D = d$ for odd D (with $d \equiv 1 \bmod 4$).

Lemma 1.1. *The field K embeds as a subfield of $\mathbf{Q}(\zeta_D)$.*

Since D may be negative, we make the convention that $\mathbf{Q}(\zeta_n)$ means $\mathbf{Q}(\zeta_{|n|})$ for any nonzero integer n. For any $n < 0$ we may write $X^n - 1 = -X^n(X^{|n|} - 1)$, so we have $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$ for any nonzero $n \in \mathbf{Z}$.

Proof. First assume D is odd, so $D = d \equiv 1 \bmod 4$. Since $d \neq 1$, we have $d \neq \pm 1$ and hence $d = \pm \prod p_i$ for a non-empty finite set of pairwise distinct odd primes p_i. For each i let $q_i = (-1|p_i)p_i$, so $q_i \equiv 1 \bmod 4$ and $D = \pm \prod q_i$. Since $D, q_i \equiv 1 \bmod 4$, there is no sign discrepancy: $D = \prod q_i$. Clearly $\mathbf{Q}(\zeta_D)$ contains $\mathbf{Q}(\zeta_{p_i})$, and by Exercise 1 in Homework 5 this latter cyclotomic field contains $\mathbf{Q}(\sqrt{q_i})$. Hence, each q_i is a square in $\mathbf{Q}(\zeta_D)$, and so $D = \prod q_i$ is also a square in $\mathbf{Q}(\zeta_D)$. That is, $K = \mathbf{Q}(\sqrt{D})$ embeds into $\mathbf{Q}(\zeta_D)$.

Now assume D is even, so $D = 4d$ with a squarefree $d \equiv 2, 3 \bmod 4$. The case $d = -1$ is trivial (as $\mathbf{Q}(\sqrt{-1}) = \mathbf{Q}(\zeta_4)$), so we may assume d is a non-unit. Let $d = \pm 2^a \cdot \prod p_i$ be the prime factorization with odd positive primes p_i and $a = 0, 1$. Let $q_i = (-1|p_i)p_i$ as above, so $d = \pm 2^a \cdot \prod q_i$. The field $\mathbf{Q}(\zeta_D)$ contains $\mathbf{Q}(\zeta_{p_i})$, and hence (as above) q_i is a square in $\mathbf{Q}(\zeta_D)$. Also, since $4|D$ we see that $\mathbf{Q}(\zeta_4) = \mathbf{Q}(\sqrt{-1})$ is contained in $\mathbf{Q}(\zeta_D)$, so -1 is a square in $\mathbf{Q}(\zeta_D)$. Hence, $\pm \prod q_i$ is a square in $\mathbf{Q}(\zeta_D)$ for both signs. This settles the case of odd d, and if d is even then $8|D$ and hence $\mathbf{Q}(\zeta_D)$ contains $\mathbf{Q}(\zeta_8)$, so 2 is also a square in $\mathbf{Q}(\zeta_D)$ in such cases. Thus, d is a square in $\mathbf{Q}(\zeta_D)$ for even d as well. ∎

There is a natural isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) \simeq (\mathbf{Z}/D\mathbf{Z})^\times$ given by $\sigma \mapsto n_\sigma$ where $\sigma(\zeta) = \zeta^{n_\sigma}$ for *all* elements ζ in the cyclic group of Dth roots of unity in $\mathbf{Q}(\zeta_D)$. (Here we use that the automorphism group of a cyclic group of order D is *canonically* identified with $(\mathbf{Z}/D\mathbf{Z})^\times$ for any nonzero integer D.) By the preceding lemma, there is a natural surjection

$$\chi_K : (\mathbf{Z}/D\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q}) = \langle \pm 1 \rangle,$$

where the final equality is the unique isomorphism between cyclic groups of order 2. The problem we want to solve is this: explicitly describe χ_K.

For any nonzero integer n relatively prime to D, we shall abuse notation and write $\chi_K(n)$ to denote $\chi_K(n \bmod D)$. This is a multiplicative function on the set of nonzero integers relatively prime to D. In particular, to "know" χ_K it suffices to determine $\chi_K(p)$ for positive primes $p \nmid D$ and to determine $\chi_K(-1)$. We first address $\chi_K(-1)$. For any integer n satisfying $|n| > 2$, the field $\mathbf{Q}(\zeta_n)$ is a CM field and under the isomorphism

$$\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$$

the intrinsic complex conjugation goes over to the element $-1 \bmod n$ because $\overline{\zeta} = \zeta^{-1}$ for any root of unity ζ in $\mathbf{C}$. Thus, by the definition of χ_K we see that $\chi_K(-1) = 1$ if and only if complex conjugation on $\mathbf{Q}(\zeta_D)$ has trivial restriction on the quadratic subfield K, which is to say that K is a real quadratic field. In other words, $\chi_K(-1) = 1$ if $D > 0$ and $\chi_K(-1) = -1$ if $D < 0$. This proves:

Lemma 1.2. *For any quadratic field K with discriminant D, $\chi_K(-1) = \mathrm{sign}(D)$.*

2. Frobenius elements

Now we turn our attention to the computation of $\chi_K(p)$ for positive primes $p \nmid D$. The computation of $\chi_K(-1)$ rested on identifying the Galois automorphism $-1 \bmod D$ on $\mathbf{Q}(\zeta_D)$ with complex conjugation, and the fact that this restricts to complex conjugation on quadratic subfields. We require an analogous interpretation of $p \bmod D$ as a Galois automorphism of $\mathbf{Q}(\zeta_D)$ in a manner that is well-behaved with restriction to quadratic subfields. The interpretation will rest on Frobenius elements.

Since $p \nmid D$, $p\mathbf{Z}$ is unramified in $\mathbf{Z}[\zeta_D]$. Thus, for any $\mathfrak{p}$ over p in $\mathbf{Z}[\zeta_D]$ we get (by Exercise 4(v) in Homework 10) a canonical Frobenius element $\phi_{\mathfrak{p}|p\mathbf{Z}}$ in $\mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q})$ that generates $D(\mathfrak{p}|p\mathbf{Z}) = \mathrm{Gal}(\mathbf{Q}(\zeta_D)_{\mathfrak{p}}/\mathbf{Q}_p)$ and is *uniquely characterized* in this decomposition group via the condition that on the residue field $\kappa(\mathfrak{p})$ it induces the automorphism $x \mapsto x^{\#\kappa(p\mathbf{Z})} = x^p$. Recall the following general behavior of decomposition groups and Frobenius elements with respect to conjugation:

Lemma 2.1. *Let K'/K be a Galois extension of a global field K and let v be a non-archimedean place on K with v' a place over v on K'. For $g \in \mathrm{Gal}(K'/K)$, let $g(v')$ be the place on K' over v given by $|x'|_{g(v')} = |g^{-1}(x')|_{v'}$ (so in the case that K'/K is finite with v' arising from a prime ideal $\mathfrak{p}_{v'}$ of the integral closure of the uncompleted discrete valuation ring $\mathscr{O}_{K,v}$, $g(v')$ arises from the prime ideal $g(\mathfrak{p}_{v'})$). We have*

$$D(g(v')|v) = gD(v'|v)g^{-1},\ \ I(g(v')|v) = gI(v'|v)g^{-1},$$

and the resulting identification

$$D(g(v')|v)/I(g(v')|v) = gD(v'|v)g^{-1}/gI(v'|v)g^{-1}$$

carries $\phi(g(v')|v)$ to $g\phi(v'|v)g^{-1}$.

In particular, if $\mathrm{Gal}(K'/K)$ is abelian then the subgroups $D(v'|v)$ and $I(v'|v)$ in $\mathrm{Gal}(K'/K)$ are independent of the choice v' over v, and the element $\phi(v'|v) \in D(v'|v)/I(v'|v)$ is independent of v' over v.

Proof. This is a simple exercise in unwinding definitions, as well as using the unique characterization of the Frobenius element via its effect on residue fields. (In particular, one uses that if $q = p^a$ with $a > 0$ then the qth-power map is functorial with respect to all maps between commutative $\mathbf{F}_p$-algebras.) ∎

The most important case of Lemma 2.1 is when v is unramified in K', in which case $I(v'|v) = 1$ and hence $\phi(v'|v)$ is an element of $\mathrm{Gal}(K'/K)$ whose conjugacy class only depends on v. Due to this lemma, in the case of abelian extensions of a global field we usually write D_v, I_v, and ϕ_v rather than $D(v'|v)$, $I(v'|v)$, and $\phi(v'|v)$, and we call these respectively the *decomposition group at v*, the *inertia group at v*, and the (relative) *Frobenius element at v* in $\mathrm{Gal}(K'/K)$.

Let n be a nonzero integer. For any positive prime $p \nmid n$, we let Frob_p denote the Frobenius element at $p\mathbf{Z}$ in the abelian Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. This element fixes every prime $\mathfrak{p}$ over $p\mathbf{Z}$ and induces the pth-power automorphism on $\kappa(\mathfrak{p}) = \mathbf{Z}[\zeta_n]/\mathfrak{p}$ because $\#\kappa(p\mathbf{Z}) = p$ (since $p > 0$).

Lemma 2.2. *For any nonzero integer n and any positive prime $p \nmid n$, under the isomorphism*

$$\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$$

the Frobenius element Frob_p at the prime $p\mathbf{Z}$ goes over to $p \bmod n$.

Observe that $p \bmod n \neq -p \bmod n$ for $n > 2$, so the description of the Frobenius element as a specific residue class modulo n is sensitive to the distinction between the two generators $\pm p$ of $p\mathbf{Z}$.

Proof. By the definition of the isomorphism to $(\mathbf{Z}/n\mathbf{Z})^\times$, the automorphism σ_p giving rise to the residue class $p \bmod n$ acts on $\mathbf{Z}[\zeta_n]$ via $\zeta_n \mapsto \zeta_n^p$. We pick a prime $\mathfrak{p}$ over p and we need to show that $\sigma_p(\mathfrak{p}) = \mathfrak{p}$ and that the automorphism induced by σ_p on the finite field $\kappa(\mathfrak{p}) = \mathbf{Z}[\zeta_n]/\mathfrak{p}$ is the pth-power map. The endomorphism induced by σ_p on the $\mathbf{F}_p$-algebra $\mathbf{Z}[\zeta_n]/(p) = \mathbf{F}_p[T]/(\Phi_n(T))$ sends T to T^p, and so it must be the pth-power map. This map fixes all idempotents, and so the bijection between prime factors of (p) and primitive idempotents of $\mathbf{Z}[\zeta_n]/(p)$ implies that σ_p fixes all primes $\mathfrak{p}$ over $p\mathbf{Z}$. Moreover, on the quotient $\kappa(\mathfrak{p})$ of $\mathbf{Z}[\zeta_n]/(p)$ the automorphism induced by σ_p must clearly be the pth-power map, so $\sigma_p = \phi_{\mathfrak{p}|p\mathbf{Z}}$ as desired. ∎

To exploit the fact that the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) \simeq (\mathbf{Z}/D\mathbf{Z})^\times$ carries Frob_p to $p \bmod D$ for positive primes $p \nmid D$, we need to see how Frobenius elements behave with respect to quotients of Galois groups.

Lemma 2.3. *Let $K''/K'/K$ be a tower of finite extensions of global fields, with K'' and K' each Galois over K. If v'' on K'' is a non-archimedean place over places v' on K' and v on K, then the quotient map $\mathrm{Gal}(K''/K) \twoheadrightarrow \mathrm{Gal}(K'/K)$ carries $D(v''|v)$ onto $D(v'|v)$ and carries $I(v''|v)$ into $I(v'|v)$, with the induced map*

$$D(v''|v)/I(v''|v) \twoheadrightarrow D(v'|v)/I(v'|v)$$

carrying $\phi(v''|v)$ to $\phi(v'|v)$.

In particular, if v is unramified in K'' then $\mathrm{Gal}(K''/K) \twoheadrightarrow \mathrm{Gal}(K'/K)$ carries $\phi(v''|v)$ to $\phi(v'|v)$.

Note that we do not claim that $I(v''|v)$ maps onto $I(v''|v)$; this is related to the fact that $\kappa(v'')$ may be strictly larger than $\kappa(v')$. The final part of this lemma is sometimes referred to as the *functoriality of the Frobenius element* with respect to passage to quotients.

Proof. There is an induced tower $K''_{v''}/K'_{v'}/K_v$ of completions, and these are Galois because $K''_{v''} = K''K_v$ and $K'_{v'} = K'K_v$ (why?). Moreover, the inclusions of decomposition groups into the global Galois groups are identified with the natural maps of Galois groups

$$\mathrm{Gal}(K''_{v''}/K_v) \to \mathrm{Gal}(K''/K), \ \ \mathrm{Gal}(K'_{v'}/K_v) \to \mathrm{Gal}(K'/K),$$

and it is easy to check that the diagram

$$\begin{array}{ccc} \mathrm{Gal}(K''_{v''}/K_v) & \longrightarrow & \mathrm{Gal}(K''/K) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K'_{v'}/K_v) & \longrightarrow & \mathrm{Gal}(K'/K) \end{array}$$

commutes. The left side is surjective by Galois theory, and so $D(v''|v) \to D(v'|v)$ is surjective.

The natural surjective map $\mathrm{Gal}(K''_{v''}/K_v) \to \mathrm{Gal}(K'_{v'}/K_v)$ of Galois groups of local fields is compatible with the induced map $\mathrm{Aut}(\kappa(v'')/\kappa(v)) \to \mathrm{Aut}(\kappa(v')/\kappa(v))$ and so it carries $I(v''|v')$ into $I(v'|v)$ and identifies the induced map of quotients

$$D(v''|v)/I(v''|v) \twoheadrightarrow D(v'|v)/I(v'|v)$$

with the natural map of Galois groups

$$\mathrm{Gal}(\kappa(v'')/\kappa(v)) \twoheadrightarrow \mathrm{Gal}(\kappa(v')/\kappa(v)).$$

Hence, the desired behavior with respect to Frobenius elements is a consequence of the obvious general fact that if $k''/k'/k$ is a tower of finite fields with $q = \#k$ then the surjective map $\mathrm{Gal}(k''/k) \twoheadrightarrow \mathrm{Gal}(k'/k)$ carries the qth-power map to the qth-power map. ■

The preceding lemma implies that the natural quotient map $\mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q})$ carries Frob_p to the Frobenius element $\phi_{K,p}$ for the prime $p\mathbf{Z}$ that is unramified in K. In general, for any finite Galois extension F'/F of global fields and any non-archimedean place v' of F' that is unramified over its restriction v in F, the order of $\phi(v'|v)$ in $\mathrm{Gal}(F'/F)$ is the residual degree $f(v'|v)$ because $\phi(v'|v)$ is a generator of the cyclic group $\mathrm{Gal}(\kappa(v')/\kappa(v))$ of order $f(v'|v)$. In particular, $\phi(v'|v)$ is trivial if and only if $f(v'|v) = 1$. As a special case, if $[F' : F] = 2$ then an non-archimedean place v of F that is unramified in F' is split (resp. inert) in F' if and only if $\phi_v = 1$ (resp. $\phi_v \neq 1$). Thus, for a positive prime $p \nmid D$ we conclude that the Frobenius element $\phi_{K,p} \in \mathrm{Gal}(K/\mathbf{Q})$ is trivial (resp. non-trivial) if and only if $p\mathbf{Z}$ is split (resp. inert) in $\mathscr{O}_K$. In view of the *definition* of $\chi_K : (\mathbf{Z}/D\mathbf{Z})^\times \to \langle \pm 1 \rangle$ via Galois groups, we have proved:

Theorem 2.4. *For a positive prime $p \nmid D$, $\chi_K(p) = 1$ if and only if $p\mathbf{Z}$ is split in $\mathscr{O}_K$, and $\chi_K(p) = -1$ if and only if $p\mathbf{Z}$ is inert in $\mathscr{O}_K$.*

3. Jacobi symbols

By Homework 3, Exercise 3(*ii*), if p is odd then $p\mathbf{Z}$ is split in $\mathscr{O}_K$ if and only if $(D|p) = 1$ and $p\mathbf{Z}$ is inert in $\mathscr{O}_K$ if and only if $(D|p) = -1$. By the same exercise, if $p = 2$ (so D is odd, as $p \nmid D$, so $D \equiv 1 \bmod 4$) then $2\mathbf{Z}$ is split in $\mathscr{O}_K$ if and only if $D \equiv 1 \bmod 8$ and $2\mathbf{Z}$ is inert in $\mathscr{O}_K$ if and only if $D \equiv 5 \bmod 8$. Thus, by Theorem 2.4 we obtain:

Corollary 3.1. *For a positive odd prime $p \nmid D$, $\chi_K(p \bmod D) = (D|p)$. If D is odd then $\chi_K(2 \bmod D) = (-1)^{(D^2-1)/8}$.*

Our earlier result that $\chi_K(-1 \bmod D)$ expresses the action of complex conjugation on K is analogous to Corollary 3.1 in the sense that complex conjugation (relative to an embedding into $\mathbf{C}$) is generally considered to be the "Frobenius element" at a real place (since $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ is generated by complex conjugation).

Definition 3.2. Let N be a nonzero integer. The *Jacobi symbol* $(N|\cdot)$ is the unique $\langle\pm1\rangle$-valued totally multiplicative function on the set of nonzero integers relatively prime to D such that $(N|-1) = \mathrm{sign}(N)$, $(N|p)$ is the Legendre symbol for positive odd primes p not dividing N, and $(N|2) = (-1)^{(N^2-1)/8}$ if N is odd.

By definition, clearly $(NM|n) = (N|n)(M|n)$ for nonzero integers n, N, M with $\gcd(n, NM) = 1$. (The only part requiring a check is the case $n = 2$.) Our preceding work shows that if D is the discriminant of a quadratic field then $(D|n) = \chi_K(n \bmod D)$ for nonzero integers n relatively prime to D because both sides are totally multiplicative in n and they coincide for $n = -1$ and for $n = p$ a positive prime not dividing D. This yields a conceptual proof of a non-obvious fact that is often proved in elementary texts by tedious application of quadratic reciprocity:

Theorem 3.3. *Let N be a nonzero integer and write $N = \nu^2 N'$ with squarefree N' and $\nu \in \mathbf{Z}^+$. The Jacobi symbol $(N|n)$ only depends on $n \bmod N'$ if $N \equiv 1 \bmod 4$ and on $n \bmod 4N'$ otherwise. In particular, $(N|\cdot)$ is a well-defined quadratic character on $(\mathbf{Z}/N'\mathbf{Z})^\times$ if $N \equiv 1 \bmod 4$ and on $(\mathbf{Z}/4N'\mathbf{Z})^\times$ otherwise.*

Proof. If $N \equiv 1 \bmod 4$ then clearly $N' \equiv 1 \bmod 4$. By multiplicativity in N, we have $(N|n) = (N'|n)$ for nonzero n relatively prime to N, so we conclude that it suffices to replace N with N'. Hence, we may assume that N is squarefree. Similarly, using the the isomorphism $(\mathbf{Z}/N\mathbf{Z})^\times \simeq (\mathbf{Z}/N_1\mathbf{Z})^\times \times (\mathbf{Z}/N_2\mathbf{Z})^\times$ and the equalities $(N|n) = (N_1|n)(N_2|n)$ and $N' = N_1' N_2'$ if $N = N_1 N_2$ with $\gcd(N_1, N_2) = 1$, we may assume that $|N|$ is prime or $N = \pm1$. The cases $N = \pm1$ are trivial, so it remains to handle exactly one of the cases $N = p$ or $N = -p$ for each positive prime p. The case $N = 2$ is clear by inspection, so it suffices to treat the case $N = (-1|p)p \equiv 1 \bmod 4$ for an odd prime p. This case follows from the relationship with χ_K for the quadratic field $K = \mathbf{Q}(\sqrt{N})$ with discriminant N. ∎

We may now summarize our conclusion by means of the commutativity of the diagram:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) & \xrightarrow{\simeq} & (\mathbf{Z}/D\mathbf{Z})^\times \\ \downarrow & & \downarrow{\scriptstyle \chi_D} \\ \mathrm{Gal}(K/\mathbf{Q}) & \xrightarrow[\simeq]{} & \langle\pm1\rangle \end{array} \tag{1}$$

where $\chi_D = (D|\cdot)$ is a quadratic character on $(\mathbf{Z}/D\mathbf{Z})^\times$.

Let us conclude with an interesting refinement on the embeddability of K into $\mathbf{Q}(\zeta_D)$:

Theorem 3.4. *The cyclotomic field $\mathbf{Q}(\zeta_D)$ is the smallest one that contains K, in the sense that a cyclotomic field containing K must contain $\mathbf{Q}(\zeta_D)$.*

This theorem admits a very simple conceptual proof via local ramification considerations once the machinery of class field theory is available.

Proof. Since the intersection $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m)$ inside of an algebraic closure of $\mathbf{Q}$ is equal to $\mathbf{Q}(\zeta_{(n,m)})$ (with $n, m \in \mathbf{Z}$ nonzero), it suffices to prove that K is not contained in any proper cyclotomic subfields of $\mathbf{Q}(\zeta_D)$.

Recall that $\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_m)$ inside of an algebraic closure of $\mathbf{Q}$ if and only if either $|n| = |m|$, $|n| = 2|m|$ with odd m, or $|m| = 2|n|$ with odd n. Since D is either odd or a multiple of 4, it follows that a proper cyclotomic subfield of $\mathbf{Q}(\zeta_D)$ is precisely a cyclotomic field of the form $\mathbf{Q}(\zeta_n)$ with n a proper (possibly negative) divisor of D. It is therefore necessary and sufficient to show that the quadratic character $(D|\cdot)$ on $(\mathbf{Z}/D\mathbf{Z})^\times$ does not factor through the projection $(\mathbf{Z}/D\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/\delta\mathbf{Z})^\times$ for a proper (possibly negative) divisor δ of D. This is now a purely group-theoretic problem.

We write $D = \delta\delta'$ with $|\delta'| > 1$, and by shifting prime factors into δ we may assume δ' is prime. First assume δ' is odd, so $\gcd(\delta, \delta') = 1$. We may suppose $\delta' = (-1|p)p$ for an odd prime p, so $\delta' \equiv 1 \bmod 4$. Since $(D|\cdot) = (\delta|\cdot)(\delta'|\cdot)$ as functions on the set of integers relatively prime to D, and $(\delta|n)$ only depends on $n \bmod \delta$, we conclude that for nonzero n relatively prime to D the function $(\delta'|n)$ only depends on $n \bmod \delta$. However, since δ' is an odd prime we know that $(\delta'|n)$ also only depends on $n \bmod \delta'$. In other words, if $(D|\cdot)$ factors through $(\mathbf{Z}/\delta\mathbf{Z})^\times$ then the homomorphism $(\delta'|\cdot) : (\mathbf{Z}/D\mathbf{Z})^\times \to \langle \pm 1 \rangle$ factors through both projections

$$(\mathbf{Z}/D\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/\delta\mathbf{Z})^\times, \quad (\mathbf{Z}/D\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/\delta'\mathbf{Z})^\times,$$

and from this we seek a contradiction. Consideration of primary components of $\mathbf{Z}/D\mathbf{Z}$ shows that the kernels of these two projections generate $(\mathbf{Z}/D\mathbf{Z})^\times$ because $\gcd(\delta, \delta') = 1$, and hence $(\delta'|n) = 1$ for all n relatively prime to D. Since the map $(\mathbf{Z}/D\mathbf{Z})^\times \to (\mathbf{Z}/\delta'\mathbf{Z})^\times$ is surjective, it follows that $(\delta'|n) = 1$ for all n relatively prime to δ'. Since $\delta' = (-1|p)p \equiv 1 \bmod 4$ for an odd prime p, Jacobi reciprocity gives $(\delta'|n) = (n|\delta')$ for any odd positive integer n relatively prime to δ'. We can find such n representing any nonzero residue class modulo δ', and so in particular by taking a non-square residue class we find such n for which $(\delta'|n) = -1$. This gives a contradiction.

Now it remains to consider the case when $\delta' = \pm 2$, so in particular $D = 4d$ for a squarefree integer $d \equiv 2, 3 \bmod 4$. We have to deduce a contradiction if $(D|n)$ only depends on $n \bmod 2d$. By factoring D into a product of even and odd parts, a simple argument as above with the Chinese remainder theorem implies that if d is odd then $(-4|n)$ only depends on $n \bmod 2$ for odd n (that is, $(-4|n) = 1$ for all odd n) and that if d is even then $(8|n) = (2|n)$ only depends on $n \bmod 4$ for odd n. Since $(-4|-1) = -1$ and $(2|5) = -1$, we get a contradiction in both cases. ■

4. Application to zeta-functions

The Riemann zeta function is $\zeta(s) = \sum_{n \geq 1} n^{-s}$ for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, which is absolutely and uniformly convergent in each closed half-plane $\mathrm{Re}(s) \geq 1 + \varepsilon$ with $\varepsilon > 0$. There is also the well-known convergent Euler product $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ that is also absolutely and uniformly convergent in each closed half-plane $\mathrm{Re}(s) \geq 1 + \varepsilon$ with $\varepsilon > 0$.

On page 283 of the book "Algebraic Number Theory" by Fröhlich and Taylor, this definition is generalized to any number field K:

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} \mathrm{N}(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}$$

where the sum is taken over all nonzero ideals of $\mathscr{O}_K$ and the product is taken over all nonzero prime ideals of $\mathfrak{O}_K$. It is also proved there that these sums and products enjoy the same convergence properties as in the classical case $K = \mathbf{Q}$ (ultimately by reduction to the classical case). If K is a quadratic field with discriminant D then for $\mathrm{Re}(s) > 1$ we get the identity

$$\zeta_K(s) = \zeta(s) \cdot \prod_{p \nmid D} \left(1 - \frac{\chi_D(p \bmod D)}{p^s}\right)^{-1}$$

from comparing factors over p for all positive rational primes p, since $\chi_D(p \bmod D) = 1$ for $p\mathbf{Z}$ split in $\mathscr{O}_K$ and $\chi_D(p \bmod D) = -1$ for $p\mathbf{Z}$ inert in $\mathscr{O}_K$. We emphasize that p is always understood to denote a *positive* prime.

We can express this factorization of ζ_K in terms that are intrinsic to $\mathrm{Gal}(K/\mathbf{Q})$ as follows. We let $\psi : \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$ be the unique non-trivial character, so by the commutative diagram (1) ψ "corresponds" to χ_D via the composite surjection $(\mathbf{Z}/D\mathbf{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_D)/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q})$. Thus, if we define

$$L(s,\psi) = \prod_{p \nmid D} \left(1 - \frac{\psi(\mathrm{Frob}_{K,p})}{p^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$, with $\mathrm{Frob}_{K,p} \in \mathrm{Gal}(K/\mathbf{Q})$ denoting the Frobenius element at p, then

$$\zeta_K(s) = \zeta_{\mathbf{Q}}(s) L(s,\psi)$$

for $\mathrm{Re}(s) > 1$.