Global zeta classes and local invariants of polynomials

Lukas Prader

Abstract

To any polynomial \( f \in \mathbb{Q}[X] \) we associate an equivalence class \( Z_f \) of meromorphic functions on the half plane \( \{ s \in \mathbb{C} \mid \text{Re}(s) > 1 \} \), henceforth called the global zeta class of \( f \), which encodes the factorization behaviour of \( f \) modulo prime numbers. Then we relate analytic properties of \( Z_f \) to certain invariants (e.g., the number of irreducible factors) of the polynomial \( f \), culminating in interesting local-global principles.

1 Prologue: Irreducible polynomials that are reducible modulo every prime number

Suppose that we would like to prove that a certain monic polynomial \( f \in \mathbb{Z}[X] \) is irreducible. Then it might be insightful to consider the reduction \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) of \( f \) modulo prime numbers \( p \). Indeed, since reduction modulo \( p \) defines a ring homomorphism \( \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X] \), it is clear that \( f \) is irreducible if \( \overline{f} \) is. Further, the irreducibility of \( \overline{f} \) may be checked by brute-force search, as the number of polynomials in \( (\mathbb{Z}/p\mathbb{Z})[X] \) of any given degree is finite.

This raises the question whether it is always possible to find a prime \( p \) such that \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) is irreducible. Unfortunately, one cannot expect that in general, as was first observed by Hilbert in \([1]\). Indeed, if we restrict our attention to normal polynomials, i.e., if we require \( \mathbb{Q}[X]/(f) \) to be a Galois extension of \( \mathbb{Q} \), we obtain the following particularly nice characterization.

Proposition 1.1: Let \( f \in \mathbb{Z}[X] \) be irreducible, monic and normal, and write \( K := \mathbb{Q}[X]/(f) \). Then the following assertions are equivalent:

(i) There exists a prime number \( p \) such that \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) is irreducible.

(ii) \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) is irreducible for infinitely many prime numbers \( p \).

(iii) \( \text{Gal}(K \mid \mathbb{Q}) \) is cyclic.

Proof: If \( p \) is a prime divisor of the discriminant \( \text{disc}(f) \neq 0 \) of \( f \), then \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) is certainly reducible by Corollary A.2. Thus we may restrict to prime numbers \( p \mid \text{disc}(f) \). In this case, \([2]\text{ Thm. 4.33}\) and Proposition A.3 suggest that \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) is irreducible if and only if \( pO_K \) is a prime ideal in

\footnote{The author has been supported by the SFB 1085 “Higher Invariants”.

the ring $O_K$ of integers of $K$.
However, if $pO_K$ is a prime ideal, $\text{Gal}(K \mid \mathbb{Q})$ must be cyclic by [2, Cor. 2, p. 367]. Conversely, if $\text{Gal}(K \mid \mathbb{Q})$ is cyclic, then Cebotarev’s density theorem implies that there are infinitely many prime numbers $p$ such that $pO_K$ is a prime ideal; see [2, Thm. 7.30]. □

For instance, the $n$–th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ is irreducible modulo some prime number if and only if $\text{Gal}(\mathbb{Q}(e^{2\pi i/n}) \mid \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, hence if and only if

$$n \in \{2, 4, p^m, 2p^m \mid p > 2 \text{ prime}, m \geq 1\}$$

by [3, Thm. 8.10]. This was already known to Golomb; see [4].

Recall that any finite abelian group $G$ may be realized as the Galois group of some Galois extension $K \mid \mathbb{Q}$; for a proof we refer to [5, Thm. 5.1]. This enables us to construct irreducible polynomials $f \in \mathbb{Z}[X]$ that split into arbitrarily many factors modulo all but finitely many prime numbers.

**Corollary 1.2:** For every $m \geq 1$, there exists an irreducible, monic and normal polynomial $f \in \mathbb{Z}[X]$ such that for every prime number $p \nmid \text{disc}(f)$, the reduction $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X]$ admits at least $m$ distinct irreducible factors.

**Proof:** Let $q \geq m$ be a prime number. Given a Galois extension $K \mid \mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, we claim that the minimal polynomial $f \in \mathbb{Z}[X]$ of any $\alpha \in O_K$ satisfying $K = \mathbb{Q}(\alpha)$ has the desired property.

To this aim, let $p \nmid \text{disc}(f)$ be a prime number, and assume that $\overline{f} = \overline{f_1} \cdots \overline{f_k}$ for pairwise distinct irreducible polynomials $\overline{f_1}, \ldots, \overline{f_k} \in (\mathbb{Z}/p\mathbb{Z})[X]$. Then [2, Thm. 4.33] and [2, Thm. 4.6] suggest that

$$\deg(\overline{f_1}) = \cdots = \deg(\overline{f_k}) =: d \text{ and } k \cdot d = [K : \mathbb{Q}] = q^2.$$ 

But $\text{Gal}(K \mid \mathbb{Q})$ is not cyclic, hence $k > 1$ by Proposition 1.1. Since $q$ is prime, we conclude that $k \geq q \geq m$. □

Finally, we shall mention the following result, which was first postulated by Brandl in 1986. Proofs can be found in [6], [7] and [8].

**Theorem 1.3:** Let $n > 1$ be an integer. Then there exists a monic and irreducible polynomial $f \in \mathbb{Z}[X]$ of degree $n$ that is reducible modulo every prime number if and only if $n$ is a composite number.

In view of Proposition 1.1, the strategy of proof could be to construct for every composite $n > 1$ a non–cyclic Galois extension of degree $n$. Indeed, as demonstrated in [5], this is possible if $\gcd(n, \varphi(n)) > 1$, where $\varphi$ denotes Euler’s totient function. However, if $\gcd(n, \varphi(n)) = 1$, there is a unique group of order $n$ (namely $\mathbb{Z}/n\mathbb{Z}$) by [9], hence the approach fails. As a consequence, the polynomial $f$ in Theorem 1.3 may be chosen normal if and only if $\gcd(n, \varphi(n)) > 1$. 

2
2 Outline of this paper

Given a polynomial \( f \in \mathbb{Q}[X] \), it is not possible in general to reduce \( f \) modulo every prime number \( p \), since \( f \) may have a coefficient whose denominator is divisible by \( p \). However, for all but finitely many primes \( p \), the coefficients of \( f \) lie in the localization \( \mathbb{Z}_p \) of \( \mathbb{Z} \) at the prime ideal \( (p) = p\mathbb{Z} \). In this case, the reduction \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) of \( f \) modulo \( p \) is defined to be the image of \( f \) under \( \mathbb{Z}_p[X] \mapsto (\mathbb{Z}_p/p\mathbb{Z}_p)[X] \cong (\mathbb{Z}/p\mathbb{Z})[X] \).

Assuming that \( \overline{f} \neq 0 \), we obtain a unique factorization
\[
\overline{f} = \overline{u} \cdot \overline{f_1}^{\alpha_1} \cdots \overline{f_k}^{\alpha_k}
\]
for some \( k \geq 0 \), where \( \alpha_1, \ldots, \alpha_k \in \mathbb{Z} \) are positive integers, \( u \in \mathbb{Z} \) is relatively prime to \( p \), and \( f_1, \ldots, f_k \in \mathbb{Z}[X] \) are monic polynomials such that their reductions \( \overline{f_1}, \ldots, \overline{f_k} \in (\mathbb{Z}/p\mathbb{Z})[X] \) modulo \( p \) are irreducible and pairwise distinct. As a convention, we shall make sense of (1) also for \( \overline{f} = 0 \) by letting \( k = 0 \) and \( \overline{u} = 0 \) in this case.

**Definition 2.1:** Let \( f \in \mathbb{Q}[X] \) be a polynomial, and let \( p \) be a prime number such that \( f \in \mathbb{Z}_p[X] \subseteq \mathbb{Q}[X] \). In the notation from (1), we define the factorization pattern of \( f \) modulo \( p \) to be the multiset
\[
\{ (\alpha_1, \deg(f_1)), \ldots, (\alpha_k, \deg(f_k)) \}.
\]

In particular, \( f \in \mathbb{Z}_p[X] \) has the factorization \( \emptyset \) modulo \( p \) precisely if \( \overline{f} \in \mathbb{Z}/p\mathbb{Z} \subseteq (\mathbb{Z}/p\mathbb{Z})[X] \) is a constant polynomial.

Further, we say that \( f \) splits completely modulo \( p \) if \( \deg(f) = \deg(\overline{f}) \) and \( \deg(f_j) = 1 \) for every \( 1 \leq j \leq k \). That means, \( f \) has factorization pattern \( \{ (\alpha_1, 1), \ldots, (\alpha_k, 1) \} \) modulo \( p \) so that \( \alpha_1 + \ldots + \alpha_k = \deg(f) \).

By a (polynomial) invariant \( I \), we mean any function
\[
I : \mathbb{Q}[X] \setminus \{ 0 \} \rightarrow \mathbb{C}.
\]

For example, the degree \( f \mapsto \deg(f) \) defines a polynomial invariant.

**Definition 2.2:** We say that a polynomial invariant \( I \) is local if it satisfies the following property: If the factorization patterns of two polynomials \( f, g \in \mathbb{Q}[X] \setminus \{ 0 \} \) agree modulo all but finitely many prime numbers \( p \), then we have \( I(f) = I(g) \).

As a consequence, if \( I \) is a local invariant and \( f \in \mathbb{Q}[X] \setminus \{ 0 \} \), then
\[
I(f(X)) = I(a \cdot f(b \cdot X + c))
\]
for all \( a, b \in \mathbb{Q}^\times \), \( c \in \mathbb{Q} \).

To revisit our example, observe that the degree is a local invariant. Indeed, let \( p \) be such that \( f \in \mathbb{Z}_p[X] \) has an invertible leading coefficient, then
\[
\deg(f) = \deg(\overline{f}) = \alpha_1 \cdot \deg(f_1) + \ldots + \alpha_k \cdot \deg(f_k)
\]
is uniquely determined by the factorization pattern (2) of \( f \) modulo \( p \).

The aim of the present paper is to prove that certain polynomial invariants are local. To achieve this goal, we mimic the ingenious approach proposed by Riemann in [10] and associate to any polynomial \( f \in \mathbb{Q}[X] \) a global zeta function \( \zeta_f \) constructed as follows: Let \( \mathcal{P}_f \) be the set of all prime numbers \( p \) such that \( f \in \mathbb{Z}_p[X] \), then we define \( \zeta_f \) for suitable \( s \in \mathbb{C} \) by an Euler product

\[
\zeta_f(s) := \prod_{p \in \mathcal{P}_f} \zeta_{f,p}(s),
\]

(3)

where each Euler factor \( \zeta_{f,p} \) is supposed to encode the factorization pattern (2) of \( f \) modulo \( p \). To this aim, we let

\[
\zeta_{f,p}(s) := \prod_{j=1}^{k} \left( \frac{1}{1 - p^{-\deg(f_j)} s} \right)^{\alpha_j}.
\]

(4)

We shall prove later that \( \zeta_f(s) \) converges for \( s \in \mathbb{C}, \Re(s) > 1 \), and that \( \zeta_f \) actually defines a holomorphic function on this half–plane. The latter observation is crucial, since it enables us to apply ideas and tools from complex analysis. Indeed, it turns out that some polynomial invariants are reflected by the analytic behaviour of \( \zeta_f \). As (4) and hence (3) only depends on the factorization patterns of \( f \) modulo prime numbers, the occurring invariants are necessarily local. The following theorem illustrates this powerful principle.

**Theorem 2.3:** For every \( f \in \mathbb{Q}[X] \), the holomorphic function

\[
\zeta_f: \{ s \in \mathbb{C} \mid \Re(s) > 1 \} \to \mathbb{C}
\]

admits a meromorphic continuation to the whole complex plane \( \mathbb{C} \).

Assume further that \( f \) factors into

\[
f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}
\]

for some \( m \geq 0 \), where \( \beta_1, \ldots, \beta_m \in \mathbb{Z} \) are positive integers, \( F_1, \ldots, F_m \in \mathbb{Q}[X] \) are irreducible, monic and pairwise distinct polynomials, and \( q \in \mathbb{Q}^\times \). Then

\[
\text{ord}_{s=1} \zeta_f(s) = -(\beta_1 + \ldots + \beta_m).
\]

In particular, the number of irreducible factors of \( f \), counted with multiplicity, is a local invariant.

Since \( f \) is irreducible if and only if it has precisely one irreducible factor (again counted with multiplicity), we conclude:

**Corollary 2.4:** A polynomial \( f \in \mathbb{Q}[X] \) is irreducible if and only if \( \zeta_f \) has a simple pole at \( s = 1 \). In particular, the irreducibility of \( f \in \mathbb{Q}[X] \) is a local invariant.

---

1 "Suitable" here expresses the requirement on \( \zeta_f(s) \) to converge.
In view of the prologue, this is a truly remarkable insight. Namely, in Corollary 1.2 we constructed irreducible polynomials that have arbitrarily large factorization patterns modulo all but finitely many prime numbers. Nevertheless, Corollary 2.4 asserts that the irreducibility of \( f \in \mathbb{Q}[X] \) is uniquely determined by \( \zeta_f \), hence by the factorization patterns of \( f \) modulo primes.

In the forthcoming section, we introduce an equivalence relation \( \doteq \) on the group of non-zero meromorphic functions \( \{ s \in \mathbb{C} \mid \text{Re}(s) > 1 \} \to \mathbb{C} \) and define the global zeta class \( Z_f \) associated to \( f \) as the equivalence class of \( \zeta_f \) modulo \( \doteq \). Roughly speaking, \( \doteq \) identifies two meromorphic functions if their quotient is a finite product of Euler factors.

In particular, \( Z_f = Z_g \) whenever the factorization patterns of \( f, g \in \mathbb{Q}[X] \) agree modulo all but finitely many prime numbers. This suggests that global zeta classes are predestined for the study of local invariants of polynomials, which is the subject of the fourth section.

In the epilogue, we finally observe that factorization patterns modulo primes may be replaced by \( p \)-adic factorization patterns throughout the paper, and we draw a bridge between global zeta classes and arithmetic zeta functions, which were first studied by Serre in [11].

Acknowledgements

The author is grateful to Guido Kings and Johannes Sprang for their supportive and fruitful remarks.

3 The global zeta class \( Z_f \)

In the following, we shall abbreviate \( U := \{ s \in \mathbb{C} \mid \text{Re}(s) > 1 \} \), and denote by \( \mathcal{M}(U) \) the field of meromorphic functions on \( U \). Furthermore, we define \( \mathcal{E}(U) \) to be the subgroup of \( \mathcal{M}(U)^\times \) generated by the holomorphic functions

\[
\phi_a(s) = 1 - a^{-s}, \quad \text{where } a \in \mathbb{Z}, a \geq 2.
\]

That means, every \( \phi \in \mathcal{E}(U) \) has the shape

\[
\phi(s) = \frac{(1 - a_1^{-s}) \cdots (1 - a_l^{-s})}{(1 - b_1^{-s}) \cdots (1 - b_m^{-s})}
\]

for some integers \( a_1, \ldots, a_l, b_1, \ldots, b_m \geq 2 \). In particular, note that the Euler factor \( \zeta_{f,p} \) defined in (4) belongs to \( \mathcal{E}(U) \) for every \( f \in \mathbb{Q}[X] \) and \( p \in \mathcal{P}_f \).

By (4), it is clear that any \( \psi \in \mathcal{E}(U) \) admits a meromorphic continuation to the whole complex plane, whose zeros and poles are contained in \( i \cdot \mathbb{R} \). Observe further that \( \psi(z) \in \mathbb{Q} \) for every \( z \in \mathbb{Z} \setminus \{0\} \).

Let \( \doteq \) be the equivalence relation on \( \mathcal{M}(U)^\times \) induced by \( \mathcal{E}(U) \), i.e.,

\[
\psi \doteq \varrho :\iff \psi\varrho^{-1} \in \mathcal{E}(U)
\]

for \( \psi, \varrho \in \mathcal{M}(U)^\times \). Moreover, we denote by \( [\psi] := \psi \cdot \mathcal{E}(U) \) the equivalence class of \( \psi \in \mathcal{M}(U)^\times \) modulo \( \doteq \). Note that \( [\psi \varrho] = [\psi] \cdot [\varrho] \) for all \( \psi, \varrho \in \mathcal{M}(U)^\times \).
We say that \([\psi]\) has a certain (analytic) property if every element in \([\psi]\) satisfies this property. E.g., our previous discussion suggests that each of the following properties transfers immediately from \(\psi\) to \([\psi]\):

(i) \(\psi: U \to \mathbb{C}\) is holomorphic.

(ii) \(\psi\) admits a meromorphic continuation \(\phi: V \to \mathbb{C}\) to some open subset \(V \subseteq \mathbb{C}\) containing \(U\).

(iii) \(\text{ord}_{s_0} \psi(s) = k\) for some \(k \in \mathbb{Z}\) and \(s_0 \in V, \text{Re}(s_0) \neq 0\).

(iv) \(\psi(z) \in M\) for some integer \(z \in V \cap \mathbb{Z}, z \neq 0\) and \(\mathbb{Q}\)-module \(M \subseteq \mathbb{C}\).

Let now \(f \in \mathbb{Q}[X]\) be a polynomial, and consider its global zeta function \(\zeta_f\) constructed in (3) and (4). Indeed, we have not yet specified the domain of \(\zeta_f\).

**Lemma 3.1:** The Euler product \(\zeta_f(s)\) converges for \(s \in \mathbb{C}, \text{Re}(s) > 1\). Moreover, \(\zeta_f\) defines a holomorphic function

\[\zeta_f: \{s \in \mathbb{C} \mid \text{Re}(s) > 1\} \to \mathbb{C}.\]

**Proof:** For any \(s \in \mathbb{C}, \text{Re}(s) > 0\) and \(p \in \mathcal{P}_f\), we may estimate

\[
|\zeta_{f,p}(s)| = \prod_{j=1}^{k} \left(\frac{1}{1 - p^{-\deg(f_j/\pi)}}\right)^{\alpha_j} \leq \prod_{j=1}^{k} \left(\frac{1}{1 - p^{-\deg(f_j/\pi) \text{Re}(s)}}\right)^{\alpha_j} \\
\leq \prod_{j=1}^{k} \left(\frac{1}{1 - p^{-\text{Re}(s)}}\right)^{\alpha_j} \leq \left(\frac{1}{1 - p^{-\text{Re}(s)}}\right)^{\deg(f)} = \zeta_p(\text{Re}(s))^{\deg(f)},
\]

where \(\zeta_p(s) := (1 - p^{-s})^{-1}\) denotes the Euler factor of Riemann’s zeta function \(\zeta\) corresponding to the prime number \(p\). Now the claim follows from the respective properties of \(\zeta\); see [12, Lemma 1, p. 129] and [12, Lemma 2, p. 133]. □

This leads us to the central definition of this paper.

**Definition 3.2:** Let \(f \in \mathbb{Q}[X]\) be a polynomial. The global zeta class \(Z_f\) associated to \(f\) is defined to be the equivalence class

\[Z_f := [\zeta_f]\]

of \(\zeta_f\) modulo \(\hat{\equiv}\).

**Remark 3.3:** Suppose that the factorization patterns of \(f, g \in \mathbb{Q}[X]\) agree modulo all but finitely many prime numbers. Then \(\zeta_{f,p} = \zeta_{g,p}\) for every such prime \(p\), thus \(\zeta_{f} \equiv \zeta_{g}\) and \(Z_f = Z_g\).

In particular, this is the case if \(g = q \cdot f\) for some rational number \(q \in \mathbb{Q}^{\times}\). Hence it suffices to study global zeta classes \(Z_f\) associated to monic polynomials \(f \in \mathbb{Q}[X]\). It will be a consequence of Proposition 3.5 and Theorem 4.1 that
one could even restrict to monic polynomials \( f \in \mathbb{Z}[X] \).

To conclude this section, we shall prove that the global zeta class \( Z_f \) of an irreducible polynomial \( f \in \mathbb{Q}[X] \) contains a unique Dedekind zeta function \( \zeta_K \) associated to a (not necessarily unique; see [13]) number field \( K \).

Let us therefore recall that Dedekind’s zeta function \( \zeta_K \) associated to a number field \( K \) is defined for \( s \in U \) by an Euler product

\[
\zeta_K(s) = \prod_p \zeta_{K,p}(s)
\]

extended over all prime numbers \( p \), where the Euler factors \( \zeta_{K,p}(s) \) are constructed as follows: Denote by \( O_K \) the ring of integers in \( K \), and assume that the principal ideal \( pO_K \) admits the unique factorization \( pO_K = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) for some \( k \geq 1 \), where \( \alpha_1, \ldots, \alpha_k \in \mathbb{Z} \) are positive integers, and \( p_1, \ldots, p_k \subseteq O_K \) are non–zero prime ideals. Then each of the field extensions \( \mathbb{Z}/p\mathbb{Z} \hookrightarrow O_K/p_j \) is finite, and its degree is simply called the degree \( \deg(p_j) \) of \( p_j \). We let

\[
\zeta_{K,p}(s) := \prod_{j=1}^{k} \frac{1}{1 - p_j^{-\deg(p_j)s}}.
\]

The attentive reader will recognize that, in contrast to (4), the exponents \( \alpha_1, \ldots, \alpha_k \) in (6) do not appear in the definition of \( \zeta_{K,p}(s) \). The main reason for this is that the factorization (2) respectively (6) admits a non–trivial \( ^2 \) exponent precisely if \( p \) divides the discriminant \( \text{disc}(f) \) of \( f \) respectively the discriminant \( \Delta_K \) of \( K \), which is due to Corollary A.2 respectively [2, Cor. 1, p. 158]. However, while \( |\Delta_K| \geq 1 \) for any \( K \), it is not true in general that \( \text{disc}(f) \neq 0 \).

We shall now summarize those properties of \( \zeta_K \) that will be applied in the sequel.

**Theorem 3.4:** Let \( K \) be a number field. We denote by \( r_1 \) (respectively \( r_2 \)) the number of real (respectively pairs of complex) embeddings of \( K \), and by \( \Delta_K \) the discriminant of \( K \).

(i) (Meromorphic continuation.) \( \zeta_K \) admits a meromorphic continuation to the whole complex plane \( \mathbb{C} \). It is holomorphic on \( \mathbb{C} \setminus \{1\} \) and has a simple pole at \( s = 1 \).

(ii) (Trivial zeros.) For every non–negative integer \( z \in \mathbb{Z} \), we have that

\[
\text{ord}_{s=-z} \zeta_K(s) =
\begin{cases}
  r_1 + r_2 - 1 & \text{if } z = 0, \\
  r_1 + r_2 & \text{if } z > 0 \text{ and } 2 \mid z, \\
  r_2 & \text{if } 2 \nmid z.
\end{cases}
\]

(iii) (Siegel–Klingen.) Assume that \( K \) is totally real, i.e., that \( r_2 = 0 \). Then

\[
\zeta_K(1-z) \in \mathbb{Q} \text{ and } \zeta_K(z) \in \mathbb{Q} \cdot \pi^{\frac{1}{2}|K:\mathbb{Q}|} \cdot \Delta_K^{1/2}
\]

\(^2\)We say that an exponent is non–trivial if it is strictly greater than 1.
for every positive and even integer $z \in \mathbb{Z}$.

(iv) Let $L$ be another number field, then $\zeta_K \div \zeta_L$ implies that $\zeta_K = \zeta_L$.

For a proof of (i), we refer to [2, Thm. 7.3]. Then (ii) follows from [2, Cor. 1, p. 315], the functional equation for $\Phi$ in [2, Thm. 7.3], and the fact that the Gamma function $\Gamma$ has simple poles at non-positive integers, but does not possess any zeros. (iii) is due to [14] respectively [15]. Finally, (iv) is a consequence of [13, Thm. 1].

Proposition 3.5: Let $f \in \mathbb{Q}[X]$ be irreducible. Then there is a unique Dedekind zeta function $\zeta_K$ such that $\zeta_K \in \mathbb{Z}_f$.

Proof: Write $K := \mathbb{Q}[X]/(f)$, and let $p \in \mathcal{P}_f$ be a prime number. Then $f \in \mathbb{Z}(p)[X]$, and we shall further assume that $\text{disc}(f) \not\in p\mathbb{Z}(p)$.

Hence $f \in (\mathbb{Z}/p\mathbb{Z})[X]$ admits a unique factorization (1) with $\alpha_1 = \cdots = \alpha_k = 1$ by Corollary A.2. Moreover, recall that $\mathbb{Z}(p) = T^{-1}\mathbb{Z}$ for the multiplicatively closed subset $T := \mathbb{Z}\setminus p\mathbb{Z} \subseteq \mathbb{Z}$. Thus [16, Prop. 5.12] suggests that $S := T^{-1}O_K$ is the integral closure of $\mathbb{Z}(p)$ in $K$, where $O_K$ denotes the ring of integers in $K$.

Now we apply [2, Thm. 4.33] and Proposition A.3 to deduce that $pS = \mathfrak{P}_1 \cdots \mathfrak{P}_k$

for pairwise distinct prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_k \subseteq S$ so that $\deg(\mathfrak{P}_j) = \deg(f_j)$ for every $1 \leq j \leq k$. Abbreviating $\mathfrak{p}_j := \mathfrak{P}_j \cap O_K \subseteq O_K$, we conclude from [16, Prop. 3.11] that

$pO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_k$

and from [16, Prop. 3.3] that $\deg(\mathfrak{P}_j) = \deg(\mathfrak{p}_j)$ for each $1 \leq j \leq k$. Thus $\zeta_{f, \mathfrak{p}} = \zeta_{K, \mathfrak{p}}$ for every $p \in \mathcal{P}_f$, $\text{disc}(f) \not\in p\mathbb{Z}(p)$. But $\text{disc}(f) \not= 0$ by Corollary A.2, hence all but finitely many primes $p$ have this property, proving that $\zeta_K \div \zeta_f$.

Finally, the uniqueness of $\zeta_K$ follows from Theorem 3.4(iv). □

Conversely, any number field $K$ may be expressed as $K = \mathbb{Q}(\alpha)$ for some algebraic integer $\alpha \in O_K$. Hence $\zeta_K \in \mathbb{Z}_f$, where $f \in \mathbb{Z}[X]$ denotes the minimal polynomial of $\alpha$. This proves that Dedekind zeta functions are in one-to-one correspondence with global zeta classes associated to irreducible polynomials.

4 Local invariants of polynomials

The central result of this section is the forthcoming factorization theorem for global zeta classes.

Theorem 4.1: Let $f \in \mathbb{Q}[X]$ be a polynomial, and assume that

$$f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}$$

for some $m \geq 0$, where $\beta_1, \ldots, \beta_m \in \mathbb{Z}$ are positive integers, $F_1, \ldots, F_m \in \mathbb{Q}[X]$ are irreducible, monic and pairwise distinct polynomials, and $q \in \mathbb{Q}^\times$. Then

$$\mathbb{Z}_f = \mathbb{Z}_{F_1}^{\beta_1} \cdots \mathbb{Z}_{F_m}^{\beta_m}.$$
Proof: By Remark 3.3 and induction on \(m\), it suffices to consider the following two cases:

(i) Assume that \(f = F^\beta\) for some positive integer \(\beta \in \mathbb{Z}\) and monic polynomial \(F \in \mathbb{Q}[X]\). Then it is clear that

\[\zeta_{f,p} = \zeta_{F^\beta,p}\]

for every prime number \(p \in \mathcal{P}_f = \mathcal{P}_F\), thus \(\zeta_f = \zeta_F^\beta\) and \(Z_f = Z_F^\beta\).

(ii) Assume that \(f = F_1 \cdot F_2\), where \(F_1, F_2 \in \mathbb{Q}[X]\) are monic and relatively prime. Then Proposition A.1 asserts that \(\text{Res}(F_1, F_2) \neq 0\), hence \(F_1, F_2 \in (\mathbb{Z}/p\mathbb{Z})[X]\) are relatively prime for all but finitely many \(p \in \mathcal{P}_f = \mathcal{P}_{F_1} \cap \mathcal{P}_{F_2}\). Consequently,

\[\zeta_{f,p} = \zeta_{F_1,p} \cdot \zeta_{F_2,p}\]

for all but finitely many primes \(p\), thus we conclude that \(Z_f = Z_{F_1} \cdot Z_{F_2}\). \(\square\)

As a bottom line, \(Z_f\) factors into global zeta classes associated to irreducible polynomials, which are related to Dedekind’s zeta function by Proposition 3.5. This has several consequences:

**Corollary 4.2:** For every \(f \in \mathbb{Q}[X]\), the global zeta class \(Z_f\) admits a meromorphic continuation to the whole complex plane.

**Proof:** This is clear for \(f = 0\), hence we may write \(f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}\) as in Theorem 4.1, and let \(K_j := \mathbb{Q}[X]/(F_j)\) for every \(1 \leq j \leq m\). Then

\[\zeta_{K_1}^{\beta_1} \cdots \zeta_{K_m}^{\beta_m} \in Z_{F_1}^{\beta_1} \cdots Z_{F_m}^{\beta_m} = Z_f\]

by Proposition 3.5, and the claim follows from Theorem 3.4(i). \(\square\)

**Corollary 4.3:** Let \(f \in \mathbb{Q}[X]\) be a polynomial, and assume that

\[f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}\]

as in Theorem 4.1. Then

\[\text{ord}_{s=1} Z_f = -(\beta_1 + \cdots + \beta_m).\]

Hence the number of irreducible factors of \(f\), counted with multiplicity, is a local invariant. In particular, the irreducibility of \(f \in \mathbb{Q}[X]\) is a local invariant.

**Proof:** By Theorem 3.4(i), \(\text{ord}_{s=1} \zeta_K(s) = -1\) for every number field \(K\). In the notation from Corollary 4.2, we thus conclude that

\[\text{ord}_{s=1} Z_f = \beta_1 \cdot \text{ord}_{s=1} \zeta_{K_1}(s) + \cdots + \beta_m \cdot \text{ord}_{s=1} \zeta_{K_m}(s) = -(\beta_1 + \cdots + \beta_m)\]

as desired. \(\square\)

The forthcoming result was first proved by Schur in [17]. Before stating it,
we recall the convention that \( \text{deg}(0) = -\infty \).

**Corollary 4.4:** For any \( f \in \mathbb{Q}[X] \), we denote by \( Z_f \subseteq \mathbb{P}f \) the subset of those \( p \in \mathbb{P}f \) such that \( \overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X] \) has a zero in \( \mathbb{Z}/p\mathbb{Z} \). Then \( Z_f \) has finite cardinality if and only if \( \text{deg}(f) = 0 \).

**Proof:** If \( Z_f \) is finite, then

\[
\hat{\zeta}_f := \prod_{p \in \mathbb{P} \setminus Z_f} \zeta_{f,p} : U \to \mathbb{C}
\]

represents \( Z_f \) and has the property that

\[
\hat{\zeta}_f(s) = \prod_{k \geq 1} \frac{1}{1 - a_k^{-b_k} s}
\]

for every \( s \in U \), where \( (a_k)_{k \geq 1}, (b_k)_{k \geq 1} \) are sequences of positive integers so that \( b_k \geq 2 \) for every \( k \geq 1 \) and \( k \log(k) \ll a_k \ll k \log(k) \) as \( k \to \infty \); compare with [13, Thm. 4.5]. Therefore the series

\[
\sum_{k=1}^{\infty} a_k^{-b_k} s
\]

converges absolutely for \( s \in \mathbb{C}, \Re(s) > 1/2 \), hence the same is true for \( \hat{\zeta}_f(s) \).

In particular, this means that \( \hat{\zeta}_f(1) \neq 0 \), or equivalently, that \( \text{ord}_{s=1} Z_f = 0 \).

Thus we may complete the proof by referring to Corollary 4.3. \( \square \)

**Corollary 4.5:** Let \( f \in \mathbb{Q}[X] \) be a non–zero polynomial, and denote by \( r_1 \) (respectively \( r_2 \)) the number of real (respectively pairs of conjugate complex) zeros of \( f \), counted with multiplicity. Then for every positive integer \( z \in \mathbb{Z} \), we have

\[
\text{ord}_{s=-z} Z_f = \begin{cases} 
    r_1 + r_2 & \text{if } 2 \mid z, \\
    r_2 & \text{if } 2 \nmid z.
\end{cases}
\]

In particular, the number of real (respectively pairs of complex) zeros of \( f \), counted with multiplicity, is a local invariant.

**Proof:** By Theorem 4.1 and the additivity of \( \text{ord}_{s=-z} \), we may assume that \( f \) is irreducible. Then the number of real (respectively pairs of complex) zeros of \( f \) is precisely the number of real (respectively pairs complex) embeddings of \( K := \mathbb{Q}[X]/(f) \), hence the claim follows from Theorem 3.4(ii). \( \square \)

**Corollary 4.6:** Let \( f \in \mathbb{Q}[X] \) be a non–zero polynomial all of whose zeros are real. Assume further that

\[
f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}
\]

as in Theorem 4.1. Then for every positive and even integer \( z \in \mathbb{Z} \), we have

\[
Z_f(1 - z) \in \mathbb{Q} \text{ and } Z_f(z) \in \mathbb{Q} \cdot \pi^{z \cdot \text{deg}(f)} \cdot \text{disc} \left( \prod_{1 \leq j \leq m, \beta_j \mid \beta} F_j \right)^{1/2}.
\]
Proof: Write $K_j := \mathbb{Q}[X]/(F_j)$ for every $1 \leq j \leq m$, then

$$ Z_{F_j}(1 - z) \in \mathbb{Q} \text{ and } Z_{F_j}(z) \in \mathbb{Q} \cdot \pi^2 \cdot [K_j, \mathbb{Q}] \Delta^{1/2}_{K_j} = \mathbb{Q} \cdot \pi^2 \cdot \text{deg}(F_j) \cdot \text{disc}(F_j)^{1/2} $$

by Theorem 3.4(iii) and Proposition A.3. Now we apply Theorem 4.1 and Corollary A.2 to conclude the proof. \qed

Next, we shall prove that the splitting field $N_f$ of $f \in \mathbb{Q}[X]$ is a local invariant. This will be a consequence of the following

**Proposition 4.7:** For any $f \in \mathbb{Q}[X]$, we denote by $S_f \subseteq P_f$ the subset of those $p \in P_f$ such that $f$ splits completely modulo $p$. Then for all $f, g \in \mathbb{Q}[X] \setminus \{0\}$, the following assertions are equivalent:

(i) The symmetric difference $S_f \Delta S_g$ has finite cardinality.

(ii) The splitting fields of $f$ and $g$ are isomorphic.

Proof: Assume without loss of generality that $f$ is monic, write $f = F_1^{\alpha_1} \cdots F_m^{\alpha_m}$ as in Theorem 4.1, and let $K_j := \mathbb{Q}[X]/(F_j)$ for every $1 \leq j \leq m$. Then $S_f = S_{F_1} \cap \cdots \cap S_{F_m}$, hence [2 Thm. 4.33 and [12 Cor., p. 76] imply that, up to finitely many exceptions, $p \in S_{F_j}$ if and only if $p$ splits completely in the splitting field $N_j$ of $F_j$. However, the splitting field $N_f$ of $f$ is isomorphic to the composite field $N_1 \cdots N_m$, and by [12 Thm. 31], a prime splits completely in $N_f$ if and only if it splits completely in $N_j$ for every $1 \leq j \leq m$. Again up to a finite number of exceptions, this means that a prime number $p$ splits completely in $N_f$ if and only if $p \in S_f$. Now the claim follows from [12 Cor. 5, p. 136]. \qed

To give another application, recall that the factorization patterns of $f, g \in \mathbb{Q}[X]$ related by $g(X) := a \cdot f(b \cdot X + c) \in \mathbb{Q}[X]$ for some $a, b \in \mathbb{Q}^\times, c \in \mathbb{Q}$, agree modulo all but finitely many prime numbers. In fact, if $f, g \in \mathbb{Q}[X]$ are irreducible and of degree 2, then also the converse is true.\footnote{One cannot expect this to be valid for higher degrees; [13 p. 351] may serve as a counterexample.}

Indeed, as quadratic field extensions are necessarily normal, observe that in this case $N_f \cong \mathbb{Q}(\sqrt{D})$ for some squarefree integer $D \in \mathbb{Z} \setminus \{0, 1\}$. Assuming further that $f$ is monic, we find $a \in \mathbb{Q}, b \in \mathbb{Q}^\times$ such that $f$ is the minimal polynomial of $a + b\sqrt{D}$, hence

$$ f = X^2 - 2a \cdot X + a^2 - b^2 D, $$

and in particular,

$$ b^{-2} \cdot f(b \cdot X + a) = X^2 - D. $$

Noting finally that for every $p \in P_f$ there are precisely three possible factorization patterns modulo $p$, namely $\{(1, 1), (1, 1)\}, \{(1, 2)\} \text{ and } \{(2, 1)\}$, where the latter occurs if and only if $\text{disc}(f) \in \mathbb{F}_p$, we conclude:

**Corollary 4.8:** Let $f, g \in \mathbb{Q}[X]$ be irreducible polynomials of degree 2. Then
the following assertions are equivalent:

(i) The symmetric difference $S_f \Delta S_g$ has finite cardinality.

(ii) The factorization patterns of $f$ and $g$ agree modulo all but finitely many prime numbers.

(iii) There exist $a, b \in \mathbb{Q}^\times, c \in \mathbb{Q}$ such that

$$f(X) = a \cdot g(b \cdot X + c).$$

Eventually, we shall provide an example of a polynomial invariant which is not local. To this aim, let $f, g \in \mathbb{Z}[X]$ be monic and irreducible polynomials such that their factorization patterns agree modulo every prime number. Then Corollary A.2 suggests that $\text{disc}(f), \text{disc}(g) \neq 0$ have precisely the same prime divisors. Furthermore, by Proposition A.3, $\text{disc}(f) = q^2 \cdot \text{disc}(g)$ for some $q \in \mathbb{Q}^\times$, implying that the exponents of any prime number $p$ in the factorizations of $\text{disc}(f), \text{disc}(g)$ have the same parity. Nevertheless, it is not necessarily true that $\text{disc}(f) = \text{disc}(g)$, as the following example demonstrates.

Example 4.9: Let $f, g \in \mathbb{Z}[X]$ be given by

$$f = X^3 + 6X^2 + 9X + 1 \text{ and } g = X^3 + 18X^2 + 81X + 27.$$ 

Then $f$ and $g$ are irreducible since $\overline{f}, \overline{g} \in (\mathbb{Z}/2\mathbb{Z})[X]$ is. Further,

$$\text{disc}(f) = 3^4 \neq 3^{10} = \text{disc}(g),$$

hence it remains to prove that the factorization patterns of $f$ and $g$ coincide modulo every prime number.

To see this, assume that $\alpha \in \overline{\mathbb{Q}}$ is any zero of $f$. Then one easily checks that $g(3\alpha) = 0$, hence $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[X]/(g)$ as fields. Thus the factorization patterns of $f$ and $g$ agree modulo every prime number $p \neq 3$, which is due to [2, Thm. 4.33] and Proposition A.3. In particular, we are done by observing that

$$\overline{f} = X^3 + \overline{T} = (X + \overline{T})^3 \in (\mathbb{Z}/3\mathbb{Z})[X] \text{ and } \overline{g} = X^3 \in (\mathbb{Z}/3\mathbb{Z})[X].$$

5 Epilogue: $P$–adic factorization patterns and arithmetic zeta functions

In this final section, we would like shed some light on two less elementary aspects of local invariants and global zeta classes.

The bottom line of our first remark will be that local invariants are also ‘local’ in a $p$–adic sense. To make this precise, let $f \in \mathbb{Q}[X]$ be a polynomial, and let $p$ be a prime number. While it is not necessarily possible to reduce $f$ modulo $p$, we may always consider the unique factorization of $f \in \mathbb{Q}_p[X]$, where $\mathbb{Q}_p$ denotes the field of $p$–adic numbers. Indeed,

$$f = r \cdot G_1^{e_1} \cdots G_h^{e_h}$$

(7)
for some $h \geq 0$, where $\gamma_1, \ldots, \gamma_h \in \mathbb{Z}$ are positive integers, $G_1, \ldots, G_h \in \mathbb{Q}_p[X]$ are irreducible, monic and pairwise distinct polynomials, and $r \in \mathbb{Q}_p^\times \subseteq \mathbb{Q}_p^\times$.

We define the $p$–adic factorization pattern of $f$ to be the multiset

$$
\{(\gamma_1, \deg(G_1)), \ldots, (\gamma_h, \deg(G_h))\}. \tag{8}
$$

Analogous to (3) and (4), one could now construct Euler factors encoding these $p$–adic factorization patterns, leading to another global zeta function associated to $f$ which does not equal $\zeta_f$ in general. However, we would still arrive at the zeta class $Z_f$, which is due to the forthcoming

**Proposition 5.1:** Let $f \in \mathbb{Q}[X]$ be a polynomial. Then for all but finitely prime numbers $p$, the factorization pattern (3) of $f$ modulo $p$ coincides with the $p$–adic factorization pattern (8) of $f$.

**Proof:** As usual, we write

$$f = q \cdot F_1^{\beta_1} \cdots F_m^{\beta_m}$$

for some $m \geq 0$, where $\beta_1, \ldots, \beta_m \in \mathbb{Z}$ are positive integers, and $F_1, \ldots, F_m \in \mathbb{Q}[X]$ are irreducible, monic and pairwise distinct polynomials, and $q \in \mathbb{Q}_p^\times$.

Then by Proposition A.1, the $p$–adic factorization pattern of $f$ is the disjoint union of the $p$–adic factorization patterns of the $F_j^{\beta_j}$, where $1 \leq j \leq m$. Indeed, the same is true for the factorization pattern of $f$ modulo any $p \in \mathcal{P}_f$, provided that $p$ does not divide $\text{Res}(F_i, F_j) \neq 0$ for all $1 \leq i < j \leq m$. By the same argument as in part (i) of the proof of Theorem 4.1, we may thus assume that $f \in \mathbb{Q}[X]$ is irreducible.

Moreover, we may restrict to primes $p \in \mathcal{P}_f$ such that $\text{disc}(f) \notin p\mathbb{Z}_p$. Then the exponents in (1) and (7) are all equal to 1 by Corollary A.2, and $p$ is unramified in $K := \mathbb{Q}[X]/(f)$ by Proposition A.3. As in the proof of Proposition 3.5, we note further that the degrees of the irreducible factors in (1) are precisely the degrees of the prime ideals appearing in the factorization of $pO_K$. However, [2, Prop. 6.1] asserts that the same is true for the irreducible factors in (7). Since we excluded at most finitely many primes, this completes the proof. □

Lastly, we shall explain the relation between our global zeta classes and arithmetic zeta functions associated to certain schemes.

To this aim, let $X$ be a scheme of finite type over $\mathbb{Z}$. For every point $x \in X$, we denote by $\mathcal{R}(x)$ the residue field of the local ring $\mathcal{O}_{X,x}$. If $x \in X$ is a closed point, then $\mathcal{R}(x)$ has finite cardinality, which is due to the fact that $\mathbb{Z}[X_1, \ldots, X_n]/m$ is a finite field for every maximal ideal $m \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ and $n \geq 0$; see [16, Exer. 7.6].

In [11], Serre associates to $X$ the arithmetic zeta function

$$\zeta_X(s) := \prod_x \frac{1}{1 - |\mathcal{R}(x)|^{-s}},$$

where the product is extended over all closed points $x \in X$. In particular, he observes the following:
Theorem 5.2: Let $X$ be a scheme of finite type over $\mathbb{Z}$. Then $\zeta_X(s)$ converges for $s \in \mathbb{C}$, $\text{Re}(s) > \dim(X)$ and defines a holomorphic function on this domain. Further, $\zeta_X$ admits a meromorphic continuation to
$$\{ s \in \mathbb{C} | \text{Re}(s) > \dim(X) - 1/2 \}$$
with a pole at $s = \dim(X)$, whose order equals the number of irreducible components of $X$ of dimension $\dim(X)$.

Given any monic polynomial $f \in \mathbb{Z}[X]$, we shall consider the arithmetic zeta function $\zeta_X$ associated to the one-dimensional scheme $X = \text{Spec}(\mathbb{Z}[X]/(f))$. Denoting by $\nu: X \to \text{Spec}(\mathbb{Z})$ the unique morphism of schemes, we first observe that
$$\zeta_X(s) = \prod_p \zeta_{X,p}(s),$$
where the product is extended over all prime numbers $p$, and where
$$\zeta_{X,p}(s) := \prod_{x \in X, \nu(x) = (p)} \frac{1}{1 - |R(x)|^{-s}}.$$

For every $p$, we may describe the Euler factor $\zeta_{X,p}$ in terms of the factorization pattern (2) of $f$ modulo $p$. Indeed, the closed points $x \in X$ satisfying $\nu(x) = (p)$ correspond to the maximal ideals in $\mathbb{Z}[X]$ containing both $f$ and $p$. If $f \equiv F_{\beta_1} \cdots F_{\beta_m} \mod p$ as in (1), then [19, Ex. H, p. 74] asserts that these are precisely the maximal ideals $m_1 := (p, f_{\beta_1}), \ldots, m_k := (p, f_{\beta_k}) \subseteq \mathbb{Z}[X]$, and
$$|\mathbb{Z}[X]/m_j| = |(\mathbb{Z}/p\mathbb{Z})[X]/(F_{\beta_j})| = p^\deg(f_{\beta_j})$$
for every $1 \leq j \leq k$. Thus we conclude that
$$\zeta_{X,p}(s) = \prod_{j=1}^k \frac{1}{1 - p^{-\deg(f_{\beta_j})} s},$$
which coincides with $\zeta_{f,p}$ if $\alpha_1 = \cdots = \alpha_k = 1$. In view of Corollary 4.3, we would hence expect that the order of the pole of $\zeta_X$ at $s = 1$ equals the number of irreducible factors of $f \in \mathbb{Q}[X]$, counted without multiplicity. To show that this actually agrees with Theorem 5.2, we recall that the irreducible components of $X$ are in one-to-one correspondence with the minimal prime ideals in $\mathbb{Z}[X]/(f)$ by [16, Exer. 1.20]. Again by [17, Ex. H, p. 74], if
$$f = F_1^{\beta_1} \cdots F_m^{\beta_m}$$
for some $m \geq 0$, positive integers $\beta_1, \ldots, \beta_m \in \mathbb{Z}$, and irreducible, monic and pairwise distinct polynomials $F_1, \ldots, F_m \in \mathbb{Z}[X]$, then the latter are precisely the principal ideals in $\mathbb{Z}[X]/(f)$ generated by $F_1, \ldots, F_m$. In summary:

Proposition 5.3: Let $f \in \mathbb{Z}[X]$ be a monic polynomial, and assume that $f$
factors as in (9). Further, let \( g := F_1 \cdots F_m \in \mathbb{Z}[X] \) and \( X := \text{Spec}(\mathbb{Z}[X]/(f)) \). Then
\[
\zeta_X \in \mathbb{Z}_g.
\]
In particular, the number of irreducible factors of \( f \) and the number of real (respectively pairs of conjugate complex) zeros of \( f \), counted without multiplicity, are local invariants.

### A Appendix: Resultant and discriminant

For the convenience of the reader, we shall collect here some basic facts about resultant and discriminant of polynomials. For a precise definition of these notions, we refer to [20, p. 119].

To fix some notation, let \( R \) be an integral domain with field of fractions \( K \). Further, let \( S \) be another integral domain, and let \( \rho: R \to S \) be a ring homomorphism. We denote by \( \rho^*: R[X] \to S[X] \) the unique extension of \( \rho \) with the property that \( \rho^*(X) = X \).

**Proposition A.1:** Let \( f, g \in R[X] \) be such that \( \deg(f) \geq 1 \).

1. \[
\rho(\text{Res}(f,g)) = \text{Res}(\rho^*(f), \rho^*(g)).
\]
2. \( \text{Res}(f,g) = 0 \) if and only if \( f \) and \( g \) have a common zero in the algebraic closure \( \overline{K} \) of \( K \), hence if and only if \( f \) and \( g \) have a common factor of positive degree in \( K[X] \).

**Proof:** (i) is a direct consequence [20, Lemma 3.3.4], and the first part of (ii) follows immediately from [20, Def. 3.3.2]. Finally, if \( \alpha \in \overline{K} \) is a common zero of \( f \) and \( g \), then the minimal polynomial of \( \alpha \) over \( K \) divides both \( f \) and \( g \) in \( K[X] \). \( \square \)

**Corollary A.2:** Let \( f, g \in R[X] \) be such that \( \deg(f), \deg(g) \geq 1 \).

1. \[
\rho(\text{disc}(f)) = \text{disc}(\rho^*(f)).
\]
2. \( \text{disc}(f) = 0 \) if and only if \( f \) has a repeated zero in \( \overline{K} \). In particular, if \( f \in K[X] \) is irreducible and \( K \) is a perfect field, then \( \text{disc}(f) \neq 0 \).
3. \[
\text{disc}(fg) = \text{disc}(f) \cdot \text{disc}(g) \cdot \text{Res}(f,g)^2.
\]

**Proof:** (i) and (ii) follow from [20, Def. 3.3.3] and Proposition A.1. (iii) is precisely [20, Cor. 3.3.6]. \( \square \)

**Proposition A.3:** Let \( R \subseteq \mathbb{Q} \) be a subring, let \( L \) be a number field of degree \( [L: \mathbb{Q}] = n \), and denote by \( S \) the integral closure of \( R \) in \( L \). Further, let \( \alpha \in S \) be such that \( L = \mathbb{Q}(\alpha) \), and denote by \( f \in R[X] \) its minimal polynomial.
(i) There exists \( r \in R \) such that \( \Delta_L \cdot r^2 = \text{disc}(f) \).

(ii) Let \( p \) be a prime divisor of \([S : R[\alpha]]\). Then \( \text{disc}(f) \in pR \).

**Proof:**
(i) Let \( v := (\omega_j)_{1 \leq j \leq n} \) be an integral basis for \( L | \mathbb{Q} \), and write \( w := (\alpha^j)_{0 \leq j \leq n-1} \). Since \( \bar{R} = T^{-1}\mathbb{Z} \) for some multiplicatively closed subset \( T \subseteq \mathbb{Z} \), \( v \) is also an \( R \)-basis for \( S = T^{-1}O_L \) by [16, Prop. 5.12] and [16, Prop. 3.3]. In particular, there is \( A \in \text{GL}_n(R) \) such that \( A \cdot v = w \), hence
\[
\text{disc}(f) = (-1)^n(n-1)/2 \cdot N_{L|\mathbb{Q}}(f'(\alpha)) = \text{disc}(\omega) = \det(A)^2 \cdot \text{disc}(v) = \det(A)^2 \cdot \Delta_L
\]
by [2, Prop. 2.9].

(ii) The claim is trivial if \( p \in R^\times \). Otherwise, \((p) = pR \subseteq R\) defines a prime ideal, hence [2, Lemma 4.32] asserts that \( p \) divides (in \( R \)) the norm \( N_{L|\mathbb{Q}}(f_{S|R[\alpha]}(f'(\alpha))) \) of the conductor \( f_{S|R[\alpha]} \) of the ring extension \( S | R[\alpha] \). Now the claim is a consequence of [2, Prop. 4.18] and the fact that \( N_{L|\mathbb{Q}}(f'(\alpha)) = (-1)^n(n-1)/2 \cdot \text{disc}(f) \).

\( \square \)
References

[1] D. Hilbert: Über diophantische Gleichungen. Nachr. Ges. der Wissenschaften zu Göttingen (1897), pp. 48–54

[2] W. Narkiewicz: Elementary and Analytic Theory of Algebraic Numbers. Springer-Verlag Berlin Heidelberg, 3rd ed. (2004)

[3] D. M. Burton: Elementary Number Theory. McGraw-Hill Higher Education, 6th ed. (2005)

[4] S. W. Golomb: Cyclotomic polynomials and factorization theorems. Amer. Math. Monthly 85/9 (1978), pp. 734–737

[5] G. Malle, B. H. Matzat: Inverse Galois theory. Springer Berlin Heidelberg, 2nd ed. (2018)

[6] R. Brandl: Integer polynomials that are reducible modulo all primes. Amer. Math. Monthly 93/4 (1986), pp. 286–288

[7] R. Guralnick, M. M. Schacher, J. Sonn: Irreducible polynomials which are locally reducible everywhere. Proc. Amer. Math. Soc. 133/11 (2005), pp. 3171–3177

[8] S. Gupta: Irreducible polynomials in Z[X] that are reducible modulo all primes. OJDM 9/2 (2019), pp. 52–61

[9] T. Szele: Über die endichen Ordnungszahlen, zu denen nur eine Gruppe gehört. Comment. Math. Helv. 20 (1947), pp. 265–267

[10] B. Riemann: über die Anzahl der Primzahlen unter einer gegebenen Größe. Monatsberichte der Berliner Akademie /11 (1859), pp. 671–680

[11] J.-P. Serre: Zeta and L–functions. pp. 82–92 in Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963). Harper & Row (1965)

[12] D. A. Marcus: Number Fields. Springer International Publishing, 2nd ed. (2018)

[13] R. Perlis: On the equation ζK(s) = ζK′(s). J. Number Theory 9/3 (1977), pp. 342–360

[14] C. L. Siegel: Über die analytische Theorie der quadratischen Formen. III. Ann. of Math. 38/1 (1937), pp. 212–291

[15] H. Klingen: Über die Werte der Dedekindschen Zetafunktion. Math. Ann. 145/3 (1962), pp. 265–272

[16] M. Atiyah, I.G. Macdonald: Introduction To Commutative Algebra. Westview Press (1994)

[17] I. Schur: Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. S-B Berlin. Math. Ges. 11 (1912), pp. 40–50

[18] T. M. Apostol: Introduction to Analytic Number Theory. Springer (2010)
[19] D. Mumford: *The Red Book of Varieties and Schemes*. Springer Berlin Heidelberg, 2nd ed. (1988)

[20] H. Cohen: *A course in computational algebraic number theory*. Springer, 3rd ed. (1993)

*Postal address:* Lukas Prader, Fakultät für Mathematik, Universität Regensburg, 93040 Regensburg, Germany

*E–mail address:* lukas.prader@mathematik.uni-regensburg.de