5. The ideal class group

We will now consider a class of rings which are not simple or semi-simple but which, in many respects, behave similarly to the ring $\mathbb{Z}$ of integers. For concreteness, we begin with a explicit example.

EXAMPLE 5.1 (Cyclotomic integers). We fix a prime number p and a primitive pth root of unity $\zeta_p \in \mathbb{C}$ and let $\mathbb{Q}(\zeta_p)$ be the pth cyclotomic field defined to be the subfield of $\mathbb{C}$ given by the sub-$\mathbb{Q}$-vector space spanned by the p elements $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. The family $(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1})$ of p elements in $\mathbb{Q}(\zeta_p)$ is not linearly independent over $\mathbb{Q}$, since we have the equation

$$1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0.$$

However, as first proved by Gauss, the subfamily $(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2})$ is linearly independent over $\mathbb{Q}$, and therefore, forms a basis of $\mathbb{Q}(\zeta_p)$ as a $\mathbb{Q}$-vector space. In particular, this $\mathbb{Q}$-vector space has dimension $p-1$. Now, let

$$\mathbb{Z}(\zeta_p) \subset \mathbb{Q}(\zeta_p)$$

be the subset of all $\mathbb{Z}$-linear combinations of $(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2})$. We claim that $\mathbb{Z}(\zeta_p)$ is a subring of $\mathbb{Q}(\zeta_p)$. Indeed, it suffices to show that the product of any two elements of the family $(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2})$ is in $\mathbb{Z}(\zeta_p)$, but if $0 \leq i, j < p-1$, then

$$\zeta_p^i \cdot \zeta_p^j = \begin{cases} \zeta_p^{i+j} & (0 \leqslant i+j < p-1) \\ -(1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-2}) & (i+j = p-1) \\ \zeta_p^{i+j-p} & (p \leqslant i+j) \end{cases}$$

which is in $\mathbb{Z}(\zeta_p)$ as claimed. The subring $\mathbb{Z}(\zeta_p) \subset \mathbb{Q}(\zeta_p)$ has the following further property: If $\alpha \in \mathbb{Q}(\zeta_p)$ is a root of a polynomial of the form

$$X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$$

where all coefficients a_i are integers, then $\alpha \in \mathbb{Z}(\zeta_p)$. We express this property, which was also proved first by Gauss, by saying that $\mathbb{Z}(\zeta_p) \subset \mathbb{Q}(\zeta_p)$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta_p)$. The ring $\mathbb{Z}(\zeta_p)$ is called the ring of p-cyclotomic integers.

We next recall that, by the fundamental theorem of arithmetic, every positive integer n can be written as a product of prime numbers

$$n = p_1 p_2 \ldots p_r$$

and this way of writing n is unique, up to permutation of the factors. In a general ring, it does not make sense to ask for an element to be positive, so we restate this theorem in a different way.

Let R be a ring. An element $a \in R$ is said to be a *unit* if there exists an element $b \in R$ such that $ab = 1 = ba$. We write $R^* \subset R$ for the subset of units; it forms a group with respect to multiplication. For instance, the group of units in the ring of integers $\mathbb{Z}$ is the group $\mathbb{Z}^* = \{+1, -1\}$, and the group of units in the matrix ring $M_n(R)$ is the group $M_n(R)^* = GL_n(R)$ of invertible matrices. Suppose now that the ring R is a subring of a field K; such a ring is called an *integral domain*. An element $p \in R$ is called *irreducible* if it is not zero and not a unit and if for all $a, b \in R$, $p = ab$ implies that $a \in R^*$ or $b \in R^*$. So the irreducible elements in $\mathbb{Z}$ are the integers $\pm p$, where p is a prime number.

DEFINITION 5.2. A ring R is a *unique factorization domain* if it is an integral domain and if every element $a \in R$ that is not zero and not a unit can be factored as a product of irreducible elements

$$a = p_1 p_2 \dots p_r,$$

and if the factorization is unique in the sense that if also

$$a = q_1 q_2 \dots q_s$$

is a factorization of a as a product of irreducible elements, then $r = s$ and, up to a permutation of the factors, the factor p_i is equal to the factor q_i times a unit in R.

The fundamental theorem of arithmetic is the statement that $\mathbb{Z}$ is a unique factorization domain. In 1847, Lamé and Cauchy announced proofs of Fermat's last theorem, which turned out to rely on the assumption that also $\mathbb{Z}(\zeta_p)$ is a unique factorization domain. But Kummer realized that this was a mistake, and he was able to prove that in fact $\mathbb{Z}(\zeta_p)$ is a unique factorization domain if and only if $p \leqslant 19$. We discuss Kummer's result in more detail following the modern formulation in terms of ideals due to Dedekind and Noether.

EXAMPLE 5.3 (Principal ideals). Let R be a commutative ring and let $a \in R$. The principal ideal generated by a is defined to be the subset

$$(a) = \{ab \mid b \in R\} \subset R.$$

We note that $(a) \subset (b)$ if and only if b divides a in the sense that $a = bc$ for some $c \in R$. In particular, we have $(a) = (b)$ is and only if a is equal to b times a unit in R. It follows that for R an integral domain, an element $p \in R$ is irreducible if and only if (p) is maximal among proper principal ideals of R. Here, an ideal $I \subset R$ is said to be proper if I is not equal to R.

DEFINITION 5.4. Let R be a commutative ring.

(i) The *product* of the ideals $\mathfrak{a}, \mathfrak{b} \subset R$ is the ideal $\mathfrak{ab} \subset R$ that consists of all sums of the form $x_1 y_1 + \dots + x_n y_n$ with $x_1, \dots, x_n \in \mathfrak{a}$, $y_1, \dots, y_n \in \mathfrak{b}$, and n a non-negative integer.

(ii) A proper ideal $\mathfrak{p} \subset R$ is a *prime ideal* if whenever $\mathfrak{p}$ contains a product $\mathfrak{ab}$ of two ideals $\mathfrak{a}, \mathfrak{b} \subset R$, then $\mathfrak{p}$ contains $\mathfrak{a}$ or $\mathfrak{p}$ contains $\mathfrak{b}$.

(iii) A proper ideal $\mathfrak{m} \subset R$ is a *maximal ideal* if it is maximal among proper ideals of R.

EXERCISE 5.5. Let R be a commutative ring. Show that a proper ideal $\mathfrak{p} \subset R$ is a prime ideal if and only if for all $a, b \in R$, $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ of $b \in \mathfrak{p}$.

LEMMA 5.6. *Let R be a commutative ring.*

(i) *Every maximal ideal $\mathfrak{m} \subset R$ is a prime ideal.*

(ii) *For every proper ideal $\mathfrak{a} \subset R$, there exists a maximal ideal $\mathfrak{m} \subset R$ with $\mathfrak{a} \subset \mathfrak{m}$.*

PROOF. (i) Let $\mathfrak{a}, \mathfrak{b} \subset R$ be two ideals such that $\mathfrak{a} \not\subset \mathfrak{m}$ and $\mathfrak{b} \not\subset \mathfrak{m}$. It suffices to show that also $\mathfrak{ab} \not\subset \mathfrak{m}$, and to this end we consider the ideal $\mathfrak{a} + \mathfrak{m} \subset R$. Since $\mathfrak{m} \subset \mathfrak{a} + \mathfrak{m}$ and since $\mathfrak{m}$ is maximal, we have either $\mathfrak{a} + \mathfrak{m} = \mathfrak{m}$ or $\mathfrak{a} + \mathfrak{m} = (1)$. But $\mathfrak{a} \subset \mathfrak{a} + \mathfrak{m}$ and $\mathfrak{a} \not\subset \mathfrak{m}$, so we conclude that $\mathfrak{a} + \mathfrak{m} = (1)$. It follows that $\mathfrak{b} = \mathfrak{ab} + \mathfrak{mb}$. Since $\mathfrak{mb} \subset \mathfrak{m}$ and since $\mathfrak{b} \not\subset \mathfrak{m}$, we conclude that $\mathfrak{ab} \not\subset \mathfrak{m}$ as desired. So $\mathfrak{m}$ is a prime ideal.

(ii) This follows from Zorn's lemma. Indeed, let S be the set of all proper ideals $\mathfrak{b} \subset R$ such that $\mathfrak{a} \subset \mathfrak{b}$. Then $\mathfrak{a} \in S$, so S is not empty. And if $T \subset S$ is a subset totally ordered with respect to inclusion of ideals, then $\mathfrak{c} = \bigcup_{\mathfrak{b} \in T} \mathfrak{b}$ is in S and is an upper bound of T. By Zorn's lemma, the set S has a maximal element. □

REMARK 5.7. In general, a prime ideal is not necessarily a maximal ideal. For example, the zero ideal $(0) \subset \mathbb{Z}$ is a prime ideal but not a maximal ideal.

DEFINITION 5.8. An integral domain R is a *Dedekind domain* if for every pair of ideals $\mathfrak{a}, \mathfrak{b} \subset R$ such that $\mathfrak{a} \subset \mathfrak{b}$, there exists an ideal $\mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Hence, among the ideals of a Dedekind ring, to contain is to divide.

EXERCISE 5.9. Show that $\mathbb{Z}$ is a Dedekind domain. (Hint: Show that every ideal $\mathfrak{a} \subset \mathbb{Z}$ is a principal ideal, then use Example 5.3.)

One can show that the rings $\mathbb{Z}(\zeta_p)$ are Dedekind domains. In fact the following more general theorem holds.

THEOREM 5.10. *Let K be a field that contains $\mathbb{Q}$ as a subfield and suppose that the dimension of K as a $\mathbb{Q}$-vector space is finite. Let $\mathcal{O}_K \subset K$ be the integral closure of $\mathbb{Z}$ in K. Then $\mathcal{O}_K$ is a Dedekind domain.*

PROOF. See [**3**, Theorem 1.4]. □

LEMMA 5.11. *Let R be a Dedekind domain and let $\mathfrak{a}, \mathfrak{b} \subset R$ be a pair of non-zero ideals such that $\mathfrak{a} \subset \mathfrak{b}$. Then there exists a unique ideal $\mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.*

PROOF. The existence of $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ is the definition of a Dedekind domain. So suppose both $\mathfrak{c}, \mathfrak{c}' \subset R$ satisfy $\mathfrak{a} = \mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{c}'$. Since $\mathfrak{a}$ and therefore $\mathfrak{b}$ are non-zero, we can choose $b \in \mathfrak{b}$ non-zero. As $(b) \subset \mathfrak{b}$, there exists an ideal $\mathfrak{r} \subset R$ such that $(b) = \mathfrak{r}\mathfrak{b}$. It follows that $(b)\mathfrak{c} = \mathfrak{r}\mathfrak{b}\mathfrak{c} = \mathfrak{r}\mathfrak{b}\mathfrak{c}' = (b)\mathfrak{c}'$. Since R is an integral domain and $b \in R$ is non-zero, we conclude that $\mathfrak{c} = \mathfrak{c}'$ as desired. □

COROLLARY 5.12. *Let R be a Dedekind domain and let $\mathfrak{p} \subset R$ be a non-zero prime ideal. Then $\mathfrak{p}$ is a maximal ideal.*

PROOF. By Lemma 5.6 (ii), there exists a maximal ideal $\mathfrak{m} \subset R$ such that $\mathfrak{p} \subset \mathfrak{m}$, and by Lemma 5.11, we can write $\mathfrak{p} = \mathfrak{m}\mathfrak{c}$ for a unique ideal $\mathfrak{c} \subset R$. Now, since $\mathfrak{p}$ is a prime ideal, either $\mathfrak{m} \subset \mathfrak{p}$ or $\mathfrak{c} \subset \mathfrak{p}$. If $\mathfrak{c} \subset \mathfrak{p}$, then

$$\mathfrak{p} = \mathfrak{m}\mathfrak{c} \subset \mathfrak{m}\mathfrak{p} \subset \mathfrak{p}$$

and hence $\mathfrak{p} = \mathfrak{m}\mathfrak{p}$. But then Lemma 5.11 shows that $\mathfrak{m} = (1)$ which contradicts that $\mathfrak{m} \subset R$ is a proper ideal. So we conclude that $\mathfrak{m} \subset \mathfrak{p}$, and hence, $\mathfrak{p} = \mathfrak{m}$. □

We next prove the following unique factorization result for the non-zero ideals in a Dedekind domain.

PROPOSITION 5.13. *Let R be a Dedekind domain. Every non-zero ideal $\mathfrak{a} \subset R$ can be factored as a product of prime ideals*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

and this factorization is unique in the sense that if also $\mathfrak{a} = \mathfrak{q}_1 \dots \mathfrak{q}_s$ is a factorization as a product of non-zero prime ideals, then $r = s$ and, up to a permutation of the factors, the factor $\mathfrak{p}_i$ is equal to the factor $\mathfrak{q}_i$.

(We note that $\mathfrak{a} = (1)$ is considered to be the product of zero prime ideals.)

PROOF. The proof that the non-zero ideal $\mathfrak{a} \subset R$ can be factored as stated is by noetherian induction. Let $\mathfrak{a}_0 = \mathfrak{a} \subset R$ be a non-zero ideal. If $\mathfrak{a}_0 = (1)$, we are done. If not, we use Lemma 5.6 to choose a maximal ideal $\mathfrak{p}_1$ with $\mathfrak{a} \subset \mathfrak{p}_1$. Then, by Lemma 5.11, we have $\mathfrak{a}_0 = \mathfrak{p}_1\mathfrak{a}_1$ for a unique non-zero ideal $\mathfrak{a}_1 \subset R$. If $\mathfrak{a}_1 = (1)$, we are done. If not, we write $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ with $\mathfrak{p}_2$ a maximal ideal that contains $\mathfrak{a}_1$. If $\mathfrak{a}_2 = (1)$, we are done. If not, we write $\mathfrak{a}_2 = \mathfrak{p}_3\mathfrak{a}_3$ with $\mathfrak{p}_3$ a maximal ideal that contains $\mathfrak{a}_2$, and so on. If after $r \geqslant 0$ steps, we have $\mathfrak{a}_r = (1)$, then $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ as desired. Assume that such an r does not exist. Then this process produces an infinite sequence of ideals

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_r \subset \cdots$$

with $\mathfrak{a}_r$ strictly contained in $\mathfrak{a}_{r+1}$. But then the union $\mathfrak{a}_\infty = \bigcup_{r \geqslant 1} \mathfrak{a}_r \subset R$ is an ideal which cannot be generated by any finite family $(x_i)_{i \in I}$ of elements of $\mathfrak{a}_\infty$. Indeed, such a family is contained in some $\mathfrak{a}_r$; but this implies that $\mathfrak{a}_\infty = \mathfrak{a}_r$ which contradicts that $\mathfrak{a}_r$ is strictly contained in $\mathfrak{a}_{r+1}$. We claim that such an ideal $\mathfrak{a}_\infty \subset R$ does not exist; more generally, we claim that every non-zero ideal $\mathfrak{b} \subset R$ is generated by a finite family of element of $\mathfrak{b}$.[1] To prove the claim, we choose $0 \neq a \in \mathfrak{b}$ and write $(a) = \mathfrak{b}\mathfrak{c}$. Then $a = b_1c_1 + \cdots + b_nc_n$ with $b_i \in \mathfrak{b}$ and $c_i \in \mathfrak{c}$, and hence, for every $b \in \mathfrak{b}$,

$$b = ba/a = b(b_1c_1 + \cdots + b_nc_n)/a = b_1(bc_1/a) + \cdots + b_n(bc_n/a).$$

So the finite family $(b_1, \dots, b_n)$ generates $\mathfrak{b}$. Here we denote by x/a the unique element $y \in R$ such that $x = ya \in (a)$.

Finally, we prove the uniqueness statement. So we suppose that

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

are two factorizations of the non-zero ideal $\mathfrak{a}$ as a product of prime ideals and proceed by induction on $n = \max\{r, s\}$. If $n = 0$, there is nothing to prove, so we let $n > 0$ and assume, inductively, that the statement has been proved for $n-1$. We note that r and s are necessarily both positive. Since the prime ideal $\mathfrak{p}_1$ contains the product $\mathfrak{q}_1 \dots \mathfrak{q}_s$, it contains one of the factors which, after reordering, we may assume to be $\mathfrak{q}_1$. But then $\mathfrak{p}_1 = \mathfrak{q}_1$ since $\mathfrak{q}_1$ is a maximal ideal. It follows from Lemma 5.11 that $\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$. By the inductive hypothesis, we conclude that $r = s$ and that, possibly after a reordering, $\mathfrak{p}_2 = \mathfrak{q}_2, \dots, \mathfrak{p}_r = \mathfrak{q}_r$. This proves the induction step, and hence, the proposition. □

LEMMA 5.14. *Let R be a Dedekind domain and suppose that R is a unique factorization domain. Then every ideal in R is a principal ideal.*

PROOF. We first show that if $p \in R$ is an irreducible element, then $(p) \subset R$ is a prime ideal. If $a, b \in R$ and $ab \in (p)$, we must show that $a \in (p)$ or $b \in (p)$. Since R is a unique factorization domain, we can write $a = p_1 \dots p_r$ and $b = p'_1 \dots p'_s$ as products of irreducible elements. Then $ab = p_1 \dots p_r p'_1 \dots p'_s$ is a factorization of ab as a product of irreducible elements. Since $ab \in (p)$, we have $ab = pc$, for some $c \in R$. We also write $c = q_1 \dots q_t$ as a product of irreducible elements. Since

$$p_1 \dots p_r p'_1 \dots p'_s = pq_1 \dots q_t,$$

[1] The zero ideal is also generated by a finite family of elements, namely, the empty family.

the uniqueness part of Definition 5.2 implies that $(p) = (p_i)$ or $(p) = (p'_j)$ for some $i = 1, \ldots, r$ or $j = 1, \ldots, s$. It follows that $a \in (p)$ or $b \in (p)$ as desired.

We next show that every ideal $\mathfrak{a} \subset R$ is a principal ideal as stated. The zero ideal is a principal ideal, so we may assume that $\mathfrak{a}$ is non-zero. By Proposition 5.13, the ideal $\mathfrak{a}$ is equal to a finite product of non-zero prime ideals. Therefore, it will suffice to show that every non-zero prime ideal $\mathfrak{p} \subset R$ is a principal ideal. To this end, we choose a non-zero element $a \in \mathfrak{p}$. Since R is a unique factorization domain, we can write $a = p_1 p_2 \ldots p_r$ as a product of irreducible elements, and since $\mathfrak{p}$ is a prime ideal, we have $(p_i) \subset \mathfrak{p}$ for some $i = 1, 2, \ldots, r$. But (p_i) is a prime ideal and hence a maximal ideal by Lemma 5.12. Therefore, we have $(p_i) = \mathfrak{p}$ which shows that $\mathfrak{p}$ is a principal ideal as desired. □

Let R be a Dedekind domain and let $\mathfrak{a}, \mathfrak{b} \subset R$ be non-zero ideals. If there exists non-zero elements $x, y \in R$ such that $x\mathfrak{a} = y\mathfrak{b}$, we say that $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* and write $\mathfrak{a} \sim \mathfrak{b}$. The following are immediately verified.

(i) For every non-zero ideal $\mathfrak{a} \subset R$, $\mathfrak{a} \sim \mathfrak{a}$.
(ii) For all non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset R$, $\mathfrak{a} \sim \mathfrak{b}$ implies $\mathfrak{b} \sim \mathfrak{a}$.
(iii) For all non-zero ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subset R$, $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{b} \sim \mathfrak{c}$ implies $\mathfrak{a} \sim \mathfrak{c}$.

We define the *ideal class* of the non-zero ideal $\mathfrak{a} \subset R$ to be the set $[\mathfrak{a}]$ of all non-zero ideals $\mathfrak{b} \subset R$ that are equivalent to $\mathfrak{a}$. The properties (i)–(iii) imply that every non-zero ideal $\mathfrak{a} \subset R$ belongs to a unique ideal class.

Definition 5.15. The *ideal class group* of the Dedekind domain R is the set

$$\mathrm{Pic}(R) = \{[\mathfrak{a}] \mid \mathfrak{a} \subset R \text{ non-zero ideal}\}$$

equipped with the multiplication defined by $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$.

Lemma 5.16. *Let R be a Dedekind domain.*

(i) *The non-zero principal ideals form the ideal class* $[(1)]$.
(ii) *The ideal class group* $\mathrm{Pic}(R)$ *is an abelian group with* $[(1)]$ *as identity element.*

Proof. (i) First, if $a \in R$ is a non-zero element, then $1 \cdot (a) = a \cdot (1)$ which shows that $(a) \in [(1)]$. Next, if $\mathfrak{a} \subset R$ is a non-zero ideal and $\mathfrak{a} \in [(1)]$, then there exists non-zero elements $x, y \in R$ such that $x\mathfrak{a} = y(1) = (y)$. In particular, there exists $a \in \mathfrak{a}$ such that $xa = y$. Now, if $c \in \mathfrak{a}$, then $xc = yb = xab$ for some $b \in R$. Since R is an integral domain, we conclude that $c = ab$ which shows that $\mathfrak{a} = (a)$ is a principal ideal.

(ii) We have $[\mathfrak{a}] \cdot [(1)] = [\mathfrak{a}(1)] = [\mathfrak{a}]$, so $[(1)]$ is the identity element. Finally, let $\mathfrak{a} \subset R$ be a non-zero ideal, and let $a \in \mathfrak{a}$ be a non-zero element. Since $(a) \subset \mathfrak{a}$, there exists a non-zero ideal $\mathfrak{b} \subset R$ such that $\mathfrak{a}\mathfrak{b} = (a)$. But then we have

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}] = [(a)] = [(1)]$$

which shows that $[\mathfrak{b}]$ is the inverse of $[\mathfrak{a}]$. □

We conclude that the Dedekind domain R is a unique factorization domain if and only if the ideal class group $\mathrm{Pic}(R)$ is zero. In general, the group $\mathrm{Pic}(R)$ is not necessarily finite. In fact, for every abelian group A, there exists a Dedekind domain R such that $\mathrm{Pic}(R)$ is isomorphic to A. However, we have the following theorem which is not so easy to prove.

THEOREM 5.17. *Let K be a field that contains $\mathbb{Q}$ as a subfield and suppose that the dimension of K as a $\mathbb{Q}$-vector space is finite. Let $\mathcal{O}_K \subset K$ be the integral closure of $\mathbb{Z}$ in K. Then the ideal class group* $\mathrm{Pic}(\mathcal{O}_K)$ *is finite.*

PROOF. See [**2**, p. 71]. □

As mentioned earlier, Kummer showed that the ideal class group $\mathbb{Z}(\zeta_p)$ is zero if and only if $p \leqslant 19$. The question of whether or not the prime p divides the order of $\mathrm{Pic}(\mathbb{Z}(\zeta_p))$ is more delicate. We make the following definition.

DEFINITION 5.18. A prime number p is *regular* if p does not divide the order of the ideal class group of $\mathbb{Z}(\zeta_p)$; otherwise, it is *irregular*.

Kummer was able to show that for a regular prime number, the equation

$$x^p + y^p = z^p$$

does not have any solutions, where x, y, and z are positive integers. He also proved the following remarkable characterization of the regular prime numbers in terms of the Riemann zeta function $\zeta(s)$. It was proved by Euler that the value of $\zeta(s)$ for s a non-positive integer is a rational number. In fact, Euler found that

$$\zeta(1-n) = -B_n/n$$

where B_n is the nth Bernoulli-Seki number[2] defined by the series

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

We will assume that rational numbers are written in their lowest terms.

THEOREM 5.19 (Kummer). *The prime number p is irregular if and only if p divides the numerator of $\zeta(1-n)$ for some positive integer n.*

In fact, Kummer showed that the prime number p is irregular if and only if p divides the numerator of $\zeta(1-n)$ for some integer $1 \leqslant n \leqslant p-3$. The first few irregular prime numbers are 37, 59, 67, 101, 103, 131, 149, and 157. It is known that there are infinitely many irregular prime numbers, but it is not known whether or not there are infinitely many regular prime numbers. The smallest n for which the numerator of $\zeta(1-n)$ is different from 1 is $n = 12$; the numerator of $\zeta(-11)$ is the prime 691, which accordingly is irregular. The smallest n such that the smallest irregular prime number 37 divides the numerator of $\zeta(1-n)$ is $n = 32$ with

$$\zeta(-31) = \frac{7,709,321,041,217}{16,320} = \frac{37 \cdot 683 \cdot 305,065,927}{2^6 \cdot 3 \cdot 5 \cdot 17}.$$

As these examples indicate, the prime numbers that divide the numerator of $\zeta(1-n)$ increase very fast with n. By contrast, only prime numbers p with $2p-3 \leqslant n$ divide the denominator of $\zeta(1-n)$.

REMARK 5.20. Let $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$ be the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. The ring $\mathbb{Z}(\zeta_p + \zeta_p^{-1}) = \mathbb{Z}(\zeta_p) \cap \mathbb{R}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and therefore, is a Dedekind domain. The Kummer-Vandiver conjecture states that for every prime number p, the order of $\mathrm{Pic}(\mathbb{Z}(\zeta_p + \zeta_p^{-1}))$ is not

[2] We warn the reader that the definition of the number B_n varies in the literature. However, everybody agrees as to the definition of $\zeta(1-n)$.

divisible by p. The conjecture, which has many important consequences, is known to be true for $p < 163,000,000$; see [**1**]. However, it may well be false.

For more details we refer to Washington's book [**4**].

References

[1] J. P. Buhler and D. Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), 2435–2444.

[2] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42–84.

[3] J. W. Milnor, *Introduction to algebraic K-theory*, Annals of Math. Studies, vol. 72, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971.

[4] L. C. Washington, *Introduction to cyclotomic fields. Second edition*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.