Mathematica Slovaca

Miroslav Lašák

Wilson's theorem in algebraic number fields

Mathematica Slovaca, Vol. 50 (2000), No. 3, 303--314

Persistent URL: http://dml.cz/dmlcz/136779

Math. Slovaca, **50** (2000), No. 3, 303–314

Mathematica Slovaca
©2000
Mathematical Institute
Slovak Academy of Sciences

WILSON'S THEOREM IN ALGEBRAIC NUMBER FIELDS

Miroslav Laššák

(*Communicated by Stanislav Jakubec*)

ABSTRACT. In this paper a generalization of Wilson's theorem

$$(p-1)! \equiv -1 \pmod{p}, \qquad p \quad \text{a prime,}$$

in algebraic number fields is proved. Gauss [DICKSON, L. E.: *History of the Theory of Numbers, Vol. I*, Carnegie Institute, Washington, 1919] generalized this proving that the product of positive integers less than n and prime to n is congruent modulo n to -1 if $n = 4, p^m, 2p^m$, where p is an odd prime, and to $+1$ if n is not of one of these three forms. Further extensions of this result to products

$$\prod_{a \in P(e)} a, \qquad \prod_{a \in G(e)} a,$$

where $P(e)$, $G(e)$ are respectively a maximal semigroup and a maximal group in $\mathbb{Z}_n$ belonging to the idempotent e, are given in [SCHWARZ, Š.: *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395]. Extending this method based on investigation of idempotents and the structure of the maximal (semi)groups, we prove analogous theorems for the residue class ring $S/\mathfrak{I}$ of the ring of integers of an algebraic number field and give specialization to some special cases of algebraic number fields.

1. Primitive idempotents

Let R be a finite commutative ring with unit element 1 and let E be the set of its idempotents. The set E is non empty $(0, 1 \in E)$ and finite. Endowed

2000 Mathematics Subject Classification: Primary 13G05; Secondary 11A05; 11R04.
Key words: idempotent, (semi)group belonging to an idempotent, unit group, Wilson's theorem, Gaussian integer, quadratic field.

Research supported by the Grant VEGA 5124.

with operations $\wedge$, $\vee$, $'$ defined by

$$x \wedge y = xy\,,$$
$$x \vee y = x + y - xy\,,$$
$$x' = 1 - x\,,$$

E forms a Boolean algebra. Atoms of $(E, \wedge, \vee)$ are called *primitive idempotents.*

Let $\varepsilon_1, \dots, \varepsilon_r$ be all the primitive idempotents of the ring R. Then $\varepsilon_1, \dots, \varepsilon_r$ are pairwise orthogonal, i.e.

$$\varepsilon_i \varepsilon_j = 0 \qquad \text{for} \quad i \neq j\,.$$

The equation

$$\varepsilon_1 + \dots + \varepsilon_r = 1 \tag{1.1}$$

gives the Peirce decomposition of the ring R

$$R = \varepsilon_1 R \oplus \dots \oplus \varepsilon_r R\,.$$

For $0 \neq \eta \in E$

$$\eta \varepsilon_i = \begin{cases} \varepsilon_i & \text{if } \varepsilon_i \leq \eta\,, \\ 0 & \text{otherwise} \end{cases}$$

and multiplying (1.1) by η we get

$$\eta = \sum_{\substack{i=1 \\ \eta\varepsilon_i = \varepsilon_i}}^{r} \varepsilon_i\,.$$

Schwarz [Sch1981] pointed out the role of idempotents in the multiplicative structure of $\mathbb{Z}_n$ to some classical congruential results of number theory. His analysis was extended to more general rings in [LaP1996]. We refer the reader to both papers for more details. To make the reading of this paper selfcontained we summarize some results which we shall use in the rest of this paper.

Denote by $P^R(\varepsilon)$ the *maximal semigroup belonging to an idempotent* $\varepsilon \in E$, i.e. the maximal subsemigroup of the multiplicative part of the ring R containing only the idempotent ε. Similarly, denote $G^R(\varepsilon)$ the *maximal group belonging to the idempotent* ε, i.e. the maximal subsemigroup of R, which is group with unit element ε. Let $N(R)$ denote nil-radical of the ring R.

PROPOSITION 1.1. *Let $\varepsilon_1, \dots, \varepsilon_r$ be all the primitive idempotents of the ring R, and let $\eta \in E$. Then*

$$P^R(\eta) = \bigoplus_{\substack{i=1,\dots,r \\ \eta\varepsilon_i = \varepsilon_i}} G^R(\varepsilon_i) \oplus \bigoplus_{\substack{i=1,\dots,r \\ \eta\varepsilon_i = 0}} N(\varepsilon_i R) = G^R(\eta) \oplus N\big((1-\eta)R\big)\,. \tag{1.2}$$

$$G^R(\eta) = \bigoplus_{\substack{i=1,\dots,r \\ \eta\varepsilon_i = \varepsilon_i}} G^R(\varepsilon_i)\,. \tag{1.3}$$

PROPOSITION 1.2. *Let ε be a primitive idempotent of the ring R. Then*

$$\varepsilon R = G^R(\varepsilon) \cup N(\varepsilon R)$$

and this union is disjoint.

2. Algebraic number fields

Let $L = \mathbb{Q}(\alpha)$ be an algebraic number field of degree n and let $S = S^{\mathbb{Q}(\alpha)}$ be the ring of algebraic integers of L. Let $\mathfrak{I}$ be a non-zero ideal of S. Since S is a Dedekind ring, $\mathfrak{I}$ has the unique factorization (up to order)

$$\mathfrak{I} = \mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_r^{u_r},$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are distinct prime ideals of S and $u_i > 0$, $i = 1, \dots, r$.

It is known that the residue class ring $S/\mathfrak{I}$ is finite. We shall denote it by $S_\mathfrak{I}$ and its elements by $[x] = [x]_\mathfrak{I} = x + \mathfrak{I}$ for $x \in S$. The *norm* $\mathcal{N}(\mathfrak{I})$ of an ideal $\mathfrak{I}$ is defined as the cardinality of the ring $S_\mathfrak{I}$.

Let the prime ideal $\mathfrak{P}_i$ contain the ideal (p_i) with rational prime p_i and let f_i be the residual degree of $\mathfrak{P}_i$ over $\mathbb{Q}$, and e_i be the ramification index of $\mathfrak{P}_i$ over (p_i), $i = 1, \dots, r$. Then $\mathcal{N}(\mathfrak{P}_i) = p_i^{f_i}$ and

$$\mathcal{N}(\mathfrak{I}) = \mathcal{N}(\mathfrak{P}_1)^{u_1} \cdots \mathcal{N}(\mathfrak{P}_r)^{u_r} = p_1^{u_1 f_1} \cdots p_r^{u_r f_r}.$$

Denote by $\varphi(\mathfrak{I})$ the order of the group of units $G^{S_\mathfrak{I}}([1]_\mathfrak{I})$ of the ring $S_\mathfrak{I}$. Then

$$\varphi(\mathfrak{I}) = \varphi(\mathfrak{P}_1^{u_1}) \cdots \varphi(\mathfrak{P}_r^{u_r}) = \mathcal{N}(\mathfrak{I}) \cdot \prod_{i=1}^{r} \left(1 - \mathcal{N}(\mathfrak{P}_i)^{-1}\right).$$

We say that $[x] \in S_\mathfrak{I}$ *belongs to a divisor* $\mathfrak{T}$ *of* $\mathfrak{I}$ if and only if $\mathfrak{T} = \big((x), \mathfrak{I}\big)$, i.e. $\mathfrak{T}$ is equal to the greatest common divisor of the principal ideal (x) and the ideal $\mathfrak{I}$. It is well defined because the ideal $\big((x), \mathfrak{I}\big)$ does not depend on the choice of the representative of the class $[x]$. Every idempotent of $S_\mathfrak{I}$ belongs to a *unitary divisor* of $\mathfrak{I}$ (a divisor $\mathfrak{T}$ is unitary if and only if $\big(\mathfrak{T}, \frac{\mathfrak{I}}{\mathfrak{T}}\big) = (1)$) and to every unitary divisor $\mathfrak{T}$ is assigned a unique idempotent. We thus have a one-to-one correspondence between idempotents of $S_\mathfrak{I}$ and unitary divisors of $\mathfrak{I}$ and hence there are 2^r idempotents. Moreover, there are exactly r primitive idempotents $\varepsilon_1, \dots, \varepsilon_r$ with ε_i belonging to the unitary divisor $\frac{\mathfrak{I}}{\mathfrak{P}_i^{u_i}}$ (see [LaP1996] for more details).

PROPOSITION 2.1. *Let η be the idempotent of $S_{\mathfrak{J}}$ belonging to the unitary divisor $\mathfrak{T}$. Then the mapping $\Psi_\eta\colon x \mapsto \eta x$ is a ring isomorphism $S_{\frac{\mathfrak{J}}{\mathfrak{T}}} \to \eta S_{\mathfrak{J}}$ and a group isomorphism $G^{S_{\frac{\mathfrak{J}}{\mathfrak{T}}}}\big([1]_{\frac{\mathfrak{J}}{\mathfrak{T}}}\big) \to G^{\eta S_{\mathfrak{J}}}(\eta)$. Specially, for every primitive idempotent ε_i, $i = 1,\dots,r$, there is an isomorphism $\Psi_{\varepsilon_i}\colon G^{S_{\mathfrak{P}_i^{u_i}}}\big([1]_{\mathfrak{P}_i^{u_i}}\big) \to G^{S_{\mathfrak{J}}}(\varepsilon_i)$.*

We prove the following theorem.

THEOREM 2.2. *Let η be the idempotent of $S_{\mathfrak{J}}$ belonging to the unitary divisor $\mathfrak{T}$, then*

$$|G^{S_{\mathfrak{J}}}(\eta)| = \left|G^{S_{\frac{\mathfrak{J}}{\mathfrak{T}}}}\big([1]_{\frac{\mathfrak{J}}{\mathfrak{T}}}\big)\right| = \varphi\left(\frac{\mathfrak{J}}{\mathfrak{T}}\right), \tag{2.1}$$

$$\big|N\big(([1]_{\mathfrak{J}} - \eta)S_{\mathfrak{J}}\big)\big| = |N(S_{\mathfrak{T}})| = \frac{\mathcal{N}(\mathfrak{T})}{\prod\limits_{\mathfrak{P}_i | \mathfrak{T}} \mathcal{N}(\mathfrak{P}_i)}, \tag{2.2}$$

$$|P^{S_{\mathfrak{J}}}(\eta)| = \frac{\mathcal{N}(\mathfrak{J})}{\prod\limits_{i=1}^{r} \mathcal{N}(\mathfrak{P}_i)} \prod_{\mathfrak{P}_i | \frac{\mathfrak{J}}{\mathfrak{T}}} \big(\mathcal{N}(\mathfrak{P}_i) - 1\big). \tag{2.3}$$

P r o o f. (2.1) follows from Proposition 2.1. Let us prove (2.2). Since

$$N\big(([1]_{\mathfrak{J}} - \eta)S_{\mathfrak{J}}\big) = \bigoplus_{\mathfrak{P}_i | \mathfrak{T}} N(\varepsilon_i S_{\mathfrak{J}}), \qquad \varepsilon_i S_{\mathfrak{J}} \simeq S_{\mathfrak{P}_i^{u_i}},$$

we have

$$\big|N\big(([1]_{\mathfrak{J}} - \eta)S_{\mathfrak{J}}\big)\big| = \prod_{\mathfrak{P}_i | \mathfrak{T}} \big|N(S_{\mathfrak{P}_i^{u_i}})\big|.$$

Furthermore, according to Proposition 1.2,

$$S_{\mathfrak{P}_i^{u_i}} = G^{S_{\mathfrak{P}_i^{u_i}}}\big([1]_{\mathfrak{P}_i^{u_i}}\big) \cup N\big(S_{\mathfrak{P}_i^{u_i}}\big)$$

and because the union is disjoint

$$\begin{aligned}
\big|N\big(S_{\mathfrak{P}_i^{u_i}}\big)\big| &= \big|S_{\mathfrak{P}_i^{u_i}}\big| - \big|G^{S_{\mathfrak{P}_i^{u_i}}}\big([1]_{\mathfrak{P}_i^{u_i}}\big)\big| \\
&= \mathcal{N}(\mathfrak{P}_i^{u_i}) - \varphi(\mathfrak{P}_i^{u_i}) \\
&= \mathcal{N}(\mathfrak{P}_i^{u_i}) - \mathcal{N}(\mathfrak{P}_i^{u_i})\big(1 - \mathcal{N}(\mathfrak{P}_i)^{-1}\big) = \mathcal{N}(\mathfrak{P}_i^{u_i})/\mathcal{N}(\mathfrak{P}_i) \\
&= \mathcal{N}(\mathfrak{P}_i)^{u_i - 1}.
\end{aligned}$$

And finally we obtain

$$\big|N\big(([1]_{\mathfrak{J}} - \eta)S_{\mathfrak{J}}\big)\big| = \prod_{\mathfrak{P}_i | \mathfrak{T}} \mathcal{N}(\mathfrak{P}_i)^{u_i - 1} = \frac{\mathcal{N}(\mathfrak{T})}{\prod\limits_{\mathfrak{P}_i | \mathfrak{T}} \mathcal{N}(\mathfrak{P}_i)}.$$

Using (1.2) of Proposition 1.1 and (2.1), (2.2) of this theorem we obtain (2.3). This completes the proof. □

As a special case of (2.2) or (2.3) for the idempotent $\eta = [0]_{\mathfrak{J}}$ belonging to the unitary divisor $\mathfrak{T} = \mathfrak{J}$ we the obtain cardinality of the nil-radical of $S_{\mathfrak{J}}$

$$|N(S_{\mathfrak{J}})| = \frac{\mathcal{N}(\mathfrak{J})}{\prod_{i=1}^{r} \mathcal{N}(\mathfrak{P}_i)}.$$

3. Wilson's theorem

Wilson's theorem states

$$(p-1)! \equiv -1 \pmod p$$

for prime p, and rewritten in terms of the maximal group its form is

$$\prod_{a \in G^{\mathbb{Z}_p}([1])} a = [-1].$$

We can consider more generally $G^{S_{\mathfrak{J}}}(\eta)$ and $P^{S_{\mathfrak{J}}}(\eta)$ instead of $G^{\mathbb{Z}_p}([1])$, where η is an idempotent of $S_{\mathfrak{J}}$, and investigate the products

$$\prod_{a \in P^{S_{\mathfrak{J}}}(\eta)} a, \qquad \prod_{a \in G^{S_{\mathfrak{J}}}(\eta)} a.$$

The case $\eta = [0] = [0]_{\mathfrak{J}}$ is very simple. Because $[0] \in P^{S_{\mathfrak{J}}}([0])$ and $[0] \in G^{S_{\mathfrak{J}}}([0])$, we get

$$\prod_{a \in P^{S_{\mathfrak{J}}}([0])} a = \prod_{a \in G^{S_{\mathfrak{J}}}([0])} a = [0]. \tag{3.1}$$

Thus we can assume in what follows that $\eta \neq [0]$.

For every $x \in G^{S_{\mathfrak{J}}}(\eta)$ and $y \in N\big(([1]-\eta)S_{\mathfrak{J}}\big)$, (1.2) of Proposition 1.1 yields that $(x+y)\eta = x$ and consequently

$$\begin{aligned}\prod_{a \in P^{S_{\mathfrak{J}}}(\eta)} a = \prod_{a \in P^{S_{\mathfrak{J}}}(\eta)} (a\eta) &= \prod_{x \in G^{S_{\mathfrak{J}}}(\eta)} \prod_{y \in N(([1]-\eta)S_{\mathfrak{J}})} (x+y)\eta \\ &= \prod_{y \in N(([1]-\eta)S_{\mathfrak{J}})} \prod_{x \in G^{S_{\mathfrak{J}}}(\eta)} x = \Big(\prod_{x \in G^{S_{\mathfrak{J}}}(\eta)} x\Big)^{k},\end{aligned}$$

where $k = \big|N\big(([1]-\eta)S_{\mathfrak{J}}\big)\big|$.

From (1.3) of Proposition 1.1 we get

$$\prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} a = \prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} (a\eta) = \prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} \Big(\sum_{\eta\varepsilon_i=\varepsilon_i} a\varepsilon_i\Big) = \sum_{\eta\varepsilon_i=\varepsilon_i} \Big(\prod_{a\in G^{S_{\mathfrak{J}}}(\varepsilon_i)} a\Big)^{l_i},$$

where $l_i = \frac{|G^{S_{\mathfrak{J}}}(\eta)|}{|G^{S_{\mathfrak{J}}}(\varepsilon_i)|}$. These results together with Theorem 2.2 give the following theorem.

THEOREM 3.1. *Let η be the idempotent of $S_{\mathfrak{J}}$ belonging to the unitary divisor $\mathfrak{T}$. Then*

$$\prod_{a\in P^{S_{\mathfrak{J}}}(\eta)} a = \Big(\prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} a\Big)^{k}, \tag{3.2}$$

where $k = \mathcal{N}(\mathfrak{T})/\prod_{\mathfrak{P}_i|\mathfrak{T}} \mathcal{N}(\mathfrak{P}_i)$, and

$$\prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} a = \sum_{\eta\varepsilon_i=\varepsilon_i} \Big(\prod_{a\in G^{S_{\mathfrak{J}}}(\varepsilon_i)} a\Big)^{l_i}, \tag{3.3}$$

where $l_i = \varphi\Big(\frac{\mathfrak{J}}{\mathfrak{P}_i^{u_i}\mathfrak{T}}\Big)$.

To find the values

$$\prod_{a\in P^{S_{\mathfrak{J}}}(\eta)} a, \qquad \prod_{a\in G^{S_{\mathfrak{J}}}(\eta)} a$$

it is sufficient to find the value $\prod_{a\in G^{S_{\mathfrak{J}}}(\varepsilon_i)} a$ for primitive idempotents ε_i, $i = 1,\dots,r$. According to Proposition 2.1 the groups $G^{S_{\mathfrak{J}}}(\varepsilon_i)$ and $G^{S_{\mathfrak{P}_i^{u_i}}}([1]_{\mathfrak{P}_i^{u_i}})$ are isomorphic and the structure of the second group is known from [Nak1979]. We have the theorem:

THEOREM 3.2. *Let ε be a primitive idempotent of $S_{\mathfrak{J}}$ belonging to the unitary divisor $\frac{\mathfrak{J}}{\mathfrak{P}^u}$ with $\mathfrak{P}$ a prime ideal containing the ideal (p), where p is a rational prime. Let e be the ramification index of $\mathfrak{P}$ over (p), and let f be the residual degree of $\mathfrak{P}$ over $\mathbb{Q}$. Then*

$$\prod_{a\in G^{S_{\mathfrak{J}}}(\varepsilon)} a = \begin{cases} -\varepsilon & \textit{iff} \quad \begin{array}{l} p>2, \\ \textit{or} \\ p=2,\ u=2,\ f=1,\ e=1, \\ \textit{or} \\ p=2,\ u=3,\ f=1,\ e=2, \end{array} \\ (\omega+1)\varepsilon & \textit{iff} \quad p=2,\ u=2,\ f=1,\ e>1,\ \omega\in\mathfrak{P}\setminus\mathfrak{P}^2, \\ (\omega^2+1)\varepsilon & \textit{iff} \quad p=2,\ u=3,\ f=1,\ e>2,\ \omega\in\mathfrak{P}\setminus\mathfrak{P}^2, \\ \varepsilon & \textit{otherwise.} \end{cases}$$

Proof. According to [Nak1979]

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \mathbb{Z}_{p^f-1} \times \prod_{t=1}^{\infty} \underbrace{\mathbb{Z}_{p^t} \times \cdots \times \mathbb{Z}_{p^t}}_{b_u(t)}, \tag{3.4}$$

where the coefficients $b_u(t)$ are also determined in [Nak1979] (but we do not need them).

Calculating the product of elements of the group (which is a direct product of cyclic groups) gives

$$\prod_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = b$$

with the property $b^2 = [1]$. Here $b = [1]$ if and only if there is no group or there is more than one group of even order on the right hand side of (3.4). Otherwise $b \neq [1]$ (if there is just one group of even order). Note that the element b is uniquely determined. Moreover in the last case $b = [-1]$ if $[1] \neq [-1]$, i.e. if $\mathfrak{P}^u \nmid 2$.

We have the following cases:

1. $p > 2$.

In this case $\mathbb{Z}_{p^f-1}$ has even order and $\mathbb{Z}_{p^t}$ has odd one for all $t \geq 1$. Therefore we have $\prod\limits_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = [-1]$ and $\prod\limits_{a \in G^{S_{\mathfrak{I}}}(\varepsilon)} a = -\varepsilon$.

2. $p = 2$.

In case $\sum\limits_{t=1}^{\infty} b_u(t) = 1$ the group $G^{S_{\mathfrak{P}^u}}([1])$ is cyclic and according to [Nar1990; Theorem 6.2] this is possible in our case if and only if $u = 2$, $f = 1$ or $u = 3$, $f = 1$, $e > 1$. In the case $u = 2$, $f = 1$, $e = 1$ or $u = 3$, $f = 1$, $e = 2$ we have $\prod\limits_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = [-1]$ and $\prod\limits_{a \in G^{S_{\mathfrak{I}}}(\varepsilon)} a = -\varepsilon$, because $\mathfrak{P}^u \nmid 2$.

In the the case $u = 2$, $f = 1$, $e > 1$ we get $b = [\omega + 1]$ and thus $\prod\limits_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = [\omega + 1]$ and $\prod\limits_{a \in G^{S_{\mathfrak{I}}}(\varepsilon)} a = (\omega + 1)\varepsilon$.

And finally, in the case $u = 3$, $f = 1$, $e > 2$ we get $b = [\omega^2 + 1]$ and thus $\prod\limits_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = [\omega^2 + 1]$ and $\prod\limits_{a \in G^{S_{\mathfrak{I}}}(\varepsilon)} a = (\omega^2 + 1)\varepsilon$. Note that in the last two cases the result does not depend on the choice of element ω.

In the remaining cases $\prod\limits_{a \in G^{S_{\mathfrak{P}^u}}([1])} a = [1]$ and $\prod\limits_{a \in G^{S_{\mathfrak{I}}}(\varepsilon)} a = \varepsilon$. □

Let η be the idempotent of $S_{\mathfrak{I}}$ belonging to the unitary divisor $\mathfrak{T}$. Without loss of generality we can suppose

$$\frac{\mathfrak{I}}{\mathfrak{T}} = \mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_s^{u_s}, \qquad 1 \leq s \leq r.$$

Note that the case $s = 0$, i.e. $\mathfrak{T} = \mathfrak{I}$, $\eta = [0]_{\mathfrak{I}}$ is solved by (3.1). Moreover, let $p_1 = \dots = p_t = 2$, $u_1 \le \dots \le u_t$ and $p_i > 2$ for $i = t+1, \dots, s$; $t = 0$ means that $p_i > 2$ for all $i = 1, \dots, s$. The number of different prime ideals containing the ideal (2) is not greater than degree n of the number field, therefore $t \le n$.

THEOREM 3.3. *Let η be the idempotent of $S_{\mathfrak{I}}$ belonging to the unitary divisor $\mathfrak{T}$. Then*

$$\prod_{a \in G^{S_{\mathfrak{I}}}(\eta)} a = \begin{cases} -\eta & \textit{iff} \quad \begin{array}{l} u_1 = \dots = u_{s-1} = 1\,,\ t = s-1\,, \\ \textit{or} \\ u_1 = \dots = u_{s-1} = 1\,,\ u_s = 2\,,\ t = s\,, \\ \qquad f_s = 1\,,\ e_s = 1\,, \\ \textit{or} \\ u_1 = \dots = u_{s-1} = 1\,,\ u_s = 3\,,\ t = s\,, \\ \qquad f_s = 1\,,\ e_s = 2\,, \end{array} \\ (\omega+1)\eta & \textit{iff} \quad \begin{array}{l} u_1 = \dots = u_{s-1} = 1\,,\ u_s = 2\,,\ t = s\,, \\ \qquad f_s = 1\,,\ e_s > 1\,, \end{array} \\ (\omega^2+1)\eta & \textit{iff} \quad \begin{array}{l} u_1 = \dots = u_{s-1} = 1\,,\ u_s = 3\,,\ t = s\,, \\ \qquad f_s = 1\,,\ e_s > 2\,, \end{array} \\ \eta & \textit{otherwise,} \end{cases}$$

where $\omega \in \mathfrak{P}_1 \cdots \mathfrak{P}_s \setminus \mathfrak{P}_1 \cdots \mathfrak{P}_{s-1}\mathfrak{P}_s^2$.

P r o o f. From (3.3) of Theorem 3.1 it follows that

$$\prod_{a \in G^{S_{\mathfrak{I}}}(\eta)} a = \sum_{i=1}^{s} \Big(\prod_{a \in G^{S_{\mathfrak{I}}}(\varepsilon_i)} a \Big)^{l_i}\,,$$
$$l_i = \varphi\left(\frac{\mathfrak{I}}{\mathfrak{P}_i^{u_i}\mathfrak{T}}\right)\,, \qquad i = 1, \dots, s\,.$$

First we observe the parity of the exponents l_i. It is odd if and only if for all $j = 1, \dots, s$, $j \ne i$, we have $p_j = 2$, $u_j = 1$. Therefore, if $s - t \ge 2$ or $t = s - 1$ and $u_{s-1} > 1$ or $t = s$ and $u_{s-1} > 1$ (then also $u_s > 1$), then all l_i, $i = 1, \dots, s$, are even and in this case

$$\prod_{a \in G^{S_{\mathfrak{I}}}(\eta)} a = \sum_{i=1}^{s} \varepsilon_i = \eta\,.$$

There remain three cases: $t = s-1$, $u_1 = \cdots = u_{s-1} = 1$ and $t = s$, $u_1 = \ldots = u_{s-1} = 1$, $u_s > 1$ and $t = s$, $u_1 = \cdots = u_{s-1} = u_s = 1$. In first two cases l_i, $i = 1, \ldots, s-1$, are even and l_s is odd. If $\prod_{a \in G^{S_\mathfrak{J}}(\varepsilon_s)} a = \varepsilon_s$, then $\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a = \eta$. If $\prod_{a \in G^{S_\mathfrak{J}}(\varepsilon_s)} a = -\varepsilon_s$, then

$$\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a = \varepsilon_1 + \cdots + \varepsilon_{s-1} - \varepsilon_s = -\varepsilon_1 - \cdots - \varepsilon_{s-1} - \varepsilon_s = -\eta,$$

because $\varepsilon_i = -\varepsilon_i$, $i = 1, \ldots, s-1$.

If $\prod_{a \in G^{S_\mathfrak{J}}(\varepsilon_s)} a = (\omega+1)\varepsilon_s$ (where $\omega \in \mathfrak{P}_1 \cdots \mathfrak{P}_s \setminus \mathfrak{P}_1 \cdots \mathfrak{P}_{s-1}\mathfrak{P}_s^2 \subset \mathfrak{P}_s \setminus \mathfrak{P}_s^2$), then

$$\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a = \varepsilon_1 + \cdots + \varepsilon_{s-1} + (\omega+1)\varepsilon_s$$
$$= (\omega+1)\varepsilon_1 + \cdots + (\omega+1)\varepsilon_{s-1} + (\omega+1)\varepsilon_s = (\omega+1)\eta,$$

because $\omega\varepsilon_i = [0]$ for all $i = 1, \ldots, s-1$. And similarly, if $\prod_{a \in G^{S_\mathfrak{J}}(\varepsilon_s)} a = (\omega^2+1)\varepsilon_s$, then

$$\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a = \varepsilon_1 + \cdots + \varepsilon_{s-1} + (\omega^2+1)\varepsilon_s$$
$$= (\omega^2+1)\varepsilon_1 + \cdots + (\omega^2+1)\varepsilon_{s-1} + (\omega^2+1)\varepsilon_s = (\omega^2+1)\eta,$$

because $\omega^2\varepsilon_i = [0]$ for all $i = 1, \ldots, s-1$.

In the third case all l_i, $i = 1, \ldots, s$, are odd and $\prod_{a \in G^{S_\mathfrak{J}}(\varepsilon_i)} a = \varepsilon_i$ for all $i = 1, \ldots, s$, hence $\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a = \eta$.

Application of Theorem 3.2 to $G^{S_\mathfrak{J}}(\varepsilon_s)$ completes the proof. □

THEOREM 3.4. *Let η be the idempotent of $S_\mathfrak{J}$ belonging to the unitary divisor $\mathfrak{T}$. Then*

$$\prod_{a \in P^{S_\mathfrak{J}}(\eta)} a = \prod_{a \in G^{S_\mathfrak{J}}(\eta)} a,$$

except in the case $\prod_{a \in G^{S_\mathfrak{J}}(\eta)} a \neq \eta$ and $p_i = 2$, $u_i > 1$ for some $i \in \{s+1, \ldots, r\}$. In this exceptional case

$$\prod_{a \in P^{S_\mathfrak{J}}(\eta)} a = \eta.$$

P r o o f . From (3.2) of Theorem 3.1 we have

$$\prod_{a\in P^{S_{\mathfrak{I}}}(\eta)} a = \Big(\prod_{a\in G^{S_{\mathfrak{I}}}(\eta)} a\Big)^{k}\,, \qquad k=\prod_{s+1}^{r}\mathcal{N}(\mathfrak{P}_i)^{u_i-1}\,.$$

Thus we have $\prod\limits_{a\in G^{S_{\mathfrak{I}}}(\eta)} a=\eta$ for k even and $\prod\limits_{a\in G^{S_{\mathfrak{I}}}(\eta)} a = \prod\limits_{a\in G^{S_{\mathfrak{I}}}(\eta)} a$ for k odd. □

4. Special cases

In this section we will concretize the theorems proved in the previous section for some algebraic number fields.

Ring $\mathbb{Z}_n$.

In this case $S=\mathbb{Z}$, $\mathfrak{I}=(n)$, i.e. $S_{\mathfrak{I}}=\mathbb{Z}_n$.

Let $\eta=[1]$. From Theorem 3.3 we have

$$\prod_{a\in G^{\mathbb{Z}_n}([1])} a = \begin{cases} & n=4\,,\\ & \text{or}\\ [-1] \quad \text{iff} & n=p^u\,, \quad p>2\,,\ u\ge 1\,,\\ & \text{or}\\ & n=2p^u\,,\ p>2\,,\ u\ge 1\,,\\ [1] \quad \text{otherwise,} & \end{cases}$$

which gives the Gauss result.

Let the idempotent η belong to the unitary divisor t of n. Then

$$\prod_{a\in G^{\mathbb{Z}_n}(\eta)} a = \begin{cases} & \frac{n}{t}=4\,,\\ & \text{or}\\ -\eta \quad \text{iff} & \frac{n}{t}=p^u\,, \quad p>2\,,\ u\ge 1\,,\\ & \text{or}\\ & \frac{n}{t}=2p^u\,,\ p>2\,,\ u\ge 1\,,\\ \eta \quad \text{otherwise,} & \end{cases}$$

which is the result of Š. S c h w a r z in [Sch1981].

Gaussian integers.

Denote by $\mathcal{G}$ the ring of Gaussian integers and let α be a non-zero integer of $\mathcal{G}$. Then Wilson's theorem for Gaussian integers has the form

$$\prod_{a\in G^{\mathcal{G}_\alpha}([1])} a = \begin{cases} & \alpha = (1+i)^3\,, \\ & \text{or} \\ [-1] \quad \text{iff} & \alpha = \pi^u\,, \qquad\qquad \pi \neq 1+i\,,\ u \geq 1\,, \\ & \text{or} \\ & \alpha = (1+i)\pi^u\,,\ \pi \neq 1+i\,,\ u \geq 1\,, \\ [i] \quad \text{iff} & \alpha = (1+i)^2\,, \\ [1] \quad \text{otherwise}, & \end{cases}$$

where π is a prime. Note that in the case $\alpha = (1+i)^2$ we take $\omega = 1+i$ and then $[\omega+1] = [i]$.

Quadratic fields.

Let m be squarefree integer and $\mathfrak{I}$ be a non-zero ideal of the ring of integers $S = S^{\mathbb{Q}(\sqrt{m}\,)}$ of quadratic field $\mathbb{Q}(\sqrt{m}\,)$. Wilson's theorem for quadratic integers takes the form

$$\prod_{a\in G^{S_{\mathfrak{I}}}([1])} a = \begin{cases} & \mathfrak{I} = \mathfrak{P}_1^2\,, \qquad p_1 = 2\,,\ m \equiv 1 \pmod 8\,, \\ & \text{or} \\ & \mathfrak{I} = \mathfrak{P}_1^3\,, \qquad p_1 = 2\,,\ m \equiv 2,3 \pmod 4\,, \\ & \text{or} \\ & \mathfrak{I} = \mathfrak{P}_1^{u_1}\,, \qquad p_1 > 2\,,\ u_1 \geq 1\,, \\ [-1] \quad \text{iff} & \text{or} \\ & \mathfrak{I} = \mathfrak{P}_1\mathfrak{P}_2^2\,, \qquad p_1 = p_2 = 2\,,\ m \equiv 1 \pmod 8\,, \\ & \text{or} \\ & \mathfrak{I} = \mathfrak{P}_1\mathfrak{P}_2^{u_2}\,, \qquad p_1 = 2\,,\ p_2 > 2\,,\ u_2 \geq 1\,, \\ & \text{or} \\ & \mathfrak{I} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3^{u_3}\,,\ p_1 = p_2 = 2\,,\ p_3 > 2\,,\ u_3 \geq 1\,, \\ [\omega+1] \quad \text{iff} & \mathfrak{I} = \mathfrak{P}_1^2\,, \qquad \begin{matrix} p_1 = 2\,,\ m \equiv 2,3 \pmod 4, \\ \omega \in \mathfrak{P}_1 \setminus \mathfrak{P}_1^2\,, \end{matrix} \\ [1] \quad \text{otherwise}, & \end{cases}$$

where $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ are distinct prime ideals containing ideals (p_1), (p_2), (p_3) respectively, where p_1, p_2, p_3 are rational primes.

Algebraic number fields.

Finally, we have Wilson's theorem for $S = S^{\mathbb{Q}(\alpha)}$, the ring of integers of the field $\mathbb{Q}(\alpha)$ of degree n.

$$\prod_{a\in G^{S_{\mathfrak{I}}}([1])} a = \begin{cases} [-1] & \text{iff} \quad \begin{array}{ll} \mathfrak{I} = \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^2, & p_1 = \cdots = p_r = 2, \\ & f_r = 1,\ e_r = 1, \\ \text{or} & \\ \mathfrak{I} = \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^3, & p_1 = \cdots = p_r = 2, \\ & f_r = 1,\ e_r = 2, \\ \text{or} & \\ \mathfrak{I} = \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^{u_r}, & p_1 = \cdots = p_{r-1} = 2, \\ & p_r > 2,\ u_r \geq 1 \end{array} \\ [\omega+1] & \text{iff} \quad \mathfrak{I} = \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^2, \quad \begin{array}{l} p_1 = \cdots = p_r = 2, \\ f_r = 1,\ e_r > 1, \end{array} \\ [\omega^2+1] & \text{iff} \quad \mathfrak{I} = \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^3, \quad \begin{array}{l} p_1 = \cdots = p_r = 2, \\ f_r = 1,\ e_r > 2, \end{array} \\ [1] & \text{otherwise}, \end{cases}$$

where $\omega \in \mathfrak{P}_1\cdots\mathfrak{P}_r \setminus \mathfrak{P}_1\cdots\mathfrak{P}_{r-1}\mathfrak{P}_r^2$, $\mathfrak{P}_i$ are distinct prime ideals containing ideals (p_i) with residual degree f_i and ramification index e_i, $i = 1,\dots,r$.

REFERENCES

[Dic1919] DICKSON, L. E.: *History of the Theory of Numbers, Vol. I*, Carnegie Institute, Washington, 1919.

[LaP1996] LAŠŠÁK, M.—PORUBSKÝ, Š.: *Fermat-Euler theorem in algebraic number fields*, J. Number Theory **60** (1996), 254–290.

[Nak1979] NAKAGOSHI, N.: *The structure of the multiplicative group of residue classes modulo* $\mathfrak{P}_{N+1}$, Nagoya Math. J. **73** (1979), 41–60.

[Nar1990] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers* (2nd ed.), PWN, Warsaw, 1990.

[Sch1981] SCHWARZ, Š.: *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395.

Received November 17, 1998

Institute of Mathematics
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
SLOVAK REPUBLIC
E-mail: lassak@savba.sk