Subgroups of finite Abelian groups having rank two via Goursat’s lemma

László Tóth

Abstract

Using Goursat’s lemma for groups, a simple representation and the invariant factor decompositions of the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$ are deduced, where $m$ and $n$ are arbitrary positive integers. As consequences, explicit formulas for the total number of subgroups, the number of subgroups with a given invariant factor decomposition, and the number of subgroups of a given order are obtained.

2010 Mathematics Subject Classification: 20K01, 20K27, 11A25

Key Words and Phrases: cyclic group, direct product, subgroup, number of subgroups, Goursat’s lemma, finite Abelian group of rank two

1 Introduction

Let $\mathbb{Z}_m$ denote the additive group of residue classes modulo $m$ and consider the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$, where $m, n \in \mathbb{N} := \{1, 2, \ldots\}$ are arbitrary. Note that this group is isomorphic to $\mathbb{Z}_{\gcd(m,n)} \times \mathbb{Z}_{\lcm(m,n)}$. If $\gcd(m,n) = 1$, then it is cyclic, isomorphic to $\mathbb{Z}_{mn}$. If $\gcd(m,n) > 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ has rank two. We recall that a finite Abelian group of order $> 1$ has rank $r$ if it is isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, where $n_1, \ldots, n_r \in \mathbb{N} \setminus \{1\}$ and $n_j | n_{j+1}$ ($1 \leq j \leq r - 1$), which is the invariant factor decomposition of the given group. Here the number $r$ is uniquely determined and represents the minimal number of generators of the group. For general accounts on finite Abelian groups see, e.g., [10, 14].

In this paper we apply Goursat’s lemma for groups, see Section 2, to derive a simple representation and the invariant factor decompositions of the subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ (Proposition 3.1). Then, as consequences, we deduce explicit formulas for the total number of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ (Proposition 4.1), the number of its subgroups of a given order (Proposition 4.2) and the number of subgroups with a given invariant factor decomposition (Proposition 4.3). The number of cyclic subgroups (of a given order) is also treated (Propositions 4.4 and 4.5). Furthermore, in Section 5 a table for the subgroups of the group $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ is given to illustrate the applicability of our identities. These results generalize and put in more compact forms those of G. Călugăreanu [4], J. Petrillo [13] and M. Tărnăuceanu [15] obtained for $p$-groups of rank two.

Another representation of the subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ and the formulas of Propositions 4.1, 4.2 and 4.4 were also derived in [7] using different arguments. Note that in the case $m = n$ the subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$ play an important role in the field of applied time-frequency analysis (cf. [7]). See [11] for asymptotic results on the number of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$. A representation of the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ ($m, n, r \in \mathbb{N}$) and a formula for the number of its subgroups was obtained in the paper [8].
Throughout the paper we use the following additional notations: \( \tau(n) \) is the number of the positive divisors of \( n \), \( \phi \) denotes Euler’s totient function, \( \mu \) is the Möbius function, * is the Dirichlet convolution of arithmetic functions.

### 2 Goursat’s lemma for groups

Goursat’s lemma for groups ([6, p. 43–48]) can be stated as follows:

**Proposition 2.1.** Let \( G \) and \( H \) be arbitrary groups. Then there is a bijection between the set \( S \) of all subgroups of \( G \times H \) and the set \( T \) of all 5-tuples \((A, B, C, D, \Psi)\), where \( B \trianglelefteq A \leq G \), \( D \trianglelefteq C \leq H \) and \( \Psi : A/B \to C/D \) is an isomorphism (here \( \trianglelefteq \) denotes subgroup and \( \trianglelefteq \) denotes normal subgroup). More precisely, the subgroup corresponding to \((A, B, C, D, \Psi)\) is

\[ K = \{(g, h) \in A \times C : \Psi(gB) = hD\}. \]

**Corollary 2.2.** Assume that \( G \) and \( H \) are finite groups and that to a subgroup \( K \) of \( G \times H \) it corresponds in this bijection the 5-tuple \((A_K, B_K, C_K, D_K, \Psi_K)\). Then one has \(|A_K| \cdot |D_K| = |K| = |B_K| \cdot |C_K|\).

For the history, proof, discussion, applications and a generalization of Goursat’s lemma see [1, 2, 5, 9, 12, 13]. Corollary 2.2 is given in [5, Cor. 3].

### 3 Representation of the subgroups of \( \mathbb{Z}_m \times \mathbb{Z}_n \)

For every \( m, n \in \mathbb{N} \) let

\[ J_{m,n} := \{(a, b, c, d, \ell) \in \mathbb{N}^5 : a \mid m, b \mid a, c \mid n, d \mid c, a/b = c/d, \quad \ell \leq a/b, \gcd(\ell, a/b) = 1\}. \]

Note that from the condition \( a/b = c/d \) we deduce \( \text{lcm}(a, c) = \text{lcm}(a, ad/b) = \text{lcm}(ad/d, ad/b) = ad/\gcd(b, d) \). That is, \( \gcd(b, d) \mid \text{lcm}(a, c) = ad \). Also, \( \gcd(b, d) \mid \text{lcm}(a, c) \).

For \((a, b, c, d, \ell) \in J_{m,n}\) define

\[ K_{a,b,c,d,\ell} := \{(im/a, i\ell n/c + jn/d) : 0 \leq i \leq a - 1, 0 \leq j \leq d - 1\}. \]

**Proposition 3.1.** Let \( m, n \in \mathbb{N} \).

i) The map \((a, b, c, d, \ell) \mapsto K_{a,b,c,d,\ell}\) is a bijection between the set \( J_{m,n} \) and the set of subgroups of \( (\mathbb{Z}_m \times \mathbb{Z}_n, +) \).

ii) The invariant factor decomposition of the subgroup \( K_{a,b,c,d,\ell} \) is

\[ K_{a,b,c,d,\ell} \cong \mathbb{Z}_{\gcd(b, d)} \times \mathbb{Z}_{\text{lcm}(a, c)}. \]

iii) The order of the subgroup \( K_{a,b,c,d,\ell} \) is \( ad \) and its exponent is \( \text{lcm}(a, c) \).

iv) The subgroup \( K_{a,b,c,d,\ell} \) is cyclic if and only if \( \gcd(b, d) = 1 \).
The Figure represents the subgroup $K_{6,2,18,6,1}$ of $Z_{12} \times Z_{18}$. It has order 36 and is isomorphic to $Z_2 \times Z_{18}$.

Proof. i) Apply Goursat’s lemma for the groups $G = Z_m$ and $H = Z_n$. We only need the following simple additional properties: All subgroups and all quotient groups of $Z_n$ ($n \in \mathbb{N}$) are cyclic. For every $n \in \mathbb{N}$ and every $a \mid n$, $a \in \mathbb{N}$, there is precisely one (cyclic) subgroup of order $a$ of $Z_n$. The number of automorphisms of $Z_n$ is $\phi(n)$ and they can be represented as $f : Z_n \rightarrow Z_n, f(x) = \ell x$, where $1 \leq \ell \leq n$, gcd$(\ell, n) = 1$.

With the notations of Proposition 2.1, let $|A| = a$, $|B| = b$, $|C| = c$, $|D| = d$, where $a \mid m$, $b \mid a$, $c \mid n$, $d \mid c$. Writing explicitly the corresponding subgroups and quotient groups we deduce

$$A = \langle m/a \rangle = \{0, m/a, 2m/a, \ldots, (a - 1)m/a\},$$

$$B = \langle m/b \rangle = \{0, m/b, 2m/b, \ldots, (b - 1)m/b\},$$

$$A/B = \langle B \rangle = \{B, m/a + B, 2m/a + B, \ldots, (a/b - 1)m/a + B\},$$

and similarly

$$C = \langle n/c \rangle = \{0, n/c, 2n/c, \ldots, (c - 1)n/c\},$$

$$D = \langle n/d \rangle = \{0, n/d, 2n/d, \ldots, (d - 1)n/d\},$$

$$C/D = \langle D \rangle = \{D, n/c + D, 2n/c + D, \ldots, (c/d - 1)n/c + D\}.$$

Now, in the case $a/b = c/d$ the values of the automorphisms $\Psi : A/B \rightarrow C/D$ are

$$\Psi(im/a + B) = i\ell n/c + D, \quad 0 \leq i \leq a/b - 1,$$
where $1 \leq \ell \leq a/b$, $\gcd(\ell, a/b) = 1$. Using (1) we deduce that the corresponding subgroup is

$$K = \{(im/a, kn/c) \in A \times C : \Psi(im/a + B) = kn/c + D\}$$

$$= \{(im/a, kn/c) : 0 \leq i \leq a - 1, 0 \leq k \leq c - 1, i\ell n/c + D = kn/c + D\},$$

where the last condition is equivalent to $kn/c \equiv i\ell n/c \pmod{n/d}$, $k \equiv i\ell \pmod{c/d}$, that is $k = i\ell + jc/d$, $0 \leq j \leq d - 1$. Hence,

$$K = \{(im/a, (i\ell + jc/d)(n/c)) : 0 \leq i \leq a - 1, 0 \leq j \leq d - 1\},$$

and the proof of the representation formula is complete.

ii-iii) It is clear from (3) that $|K| = ad = bc$ (cf. Corollary 2.2). Next we deduce the exponent of $K_{a,b,c,d,\ell}$. According to (3) the subgroup $K_{a,b,c,d,\ell}$ is generated by the elements $(0, n/d)$ and $(m/a, \ell n/c)$. Here the order of $(0, n/d)$ is $d$. To obtain the order of $(m/a, \ell n/c)$ note the following properties:

1. $m \mid r(m/a)$ if and only if $m/\gcd(m, m/a) \mid r$ if and only if $a \mid r$, and the least such $r \in \mathbb{N}$ is $a$,

2. $n \mid t(\ell n/c)$ if and only if $n/\gcd(n, \ell n/c) \mid t$ if and only if $c/\gcd(\ell, c) \mid t$, and the least such $t \in \mathbb{N}$ is $c/\gcd(\ell, c)$.

Therefore the order of $(m/a, \ell n/c)$ is $\lcm(a, c/\gcd(\ell, c))$. We deduce that the exponent of $K_{a,b,c,d,\ell}$ is

$$\lcm\left(d, \lcm\left(a, \frac{c}{\gcd(\ell, c)}\right)\right) = \lcm\left(d, a, \frac{c}{\gcd(\ell, c)}\right)$$

$$= \lcm\left(\frac{ac}{ac/d}, \frac{ac}{c/\gcd(\ell, c)}\right) = \frac{ac}{\gcd(ac/d, c/\gcd(\ell, c))}$$

$$= \frac{ac}{\gcd(c, a\gcd(\ell, c/d))} = \frac{ac}{\gcd(a, c)} = \lcm(a,c),$$

using that $\gcd(\ell, c/d) = 1$, cf. (2).

Now $K_{a,b,c,d,\ell}$ is a subgroup of the Abelian group $\mathbb{Z}_m \times \mathbb{Z}_n$ having rank $\leq 2$. Therefore, $K_{a,b,c,d,\ell}$ has also rank $\leq 2$. That is, $K_{a,b,c,d,\ell} \simeq \mathbb{Z}_u \times \mathbb{Z}_v$ for certain $u$ and $v$, where $u \mid v$ and $uv = ad$. Hence the exponent of $K_{a,b,c,d,\ell}$ is $\lcm(u, v) = v$. We obtain $v = \lcm(a,c)$ and $u = ad/\lcm(a,c) = \gcd(b,d)$. This gives (4).

iv) Clear from ii). This follows also from a general result given in [2, Th. 4.2].

Remark 3.2. If $K_{a,b,c,d,\ell}$ is defined by

$$\{(im/a, i\ell n/c + jn/d) : 0 \leq i \leq a - 1, j_i \leq j_i + d - 1\},$$

where $j_i = -[i\ell d/c]$, then $0 \leq i\ell n/c + jn/d \leq n - 1$ for every given $i$ and $j$.

4 Number of subgroups

According to Proposition 3.1 the total number $s(m,n)$ of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ can be obtained by counting the elements of the set $J_{m,n}$. 

\[\square\]
Proposition 4.1. For every \( m, n \in \mathbb{N} \), \( s(m, n) \) is given by

\[
s(m, n) = \sum_{i \mid m, j \mid n} \gcd(i, j) \tag{5}
\]

\[
= \sum_{d \mid \gcd(m,n)} \phi(d) \tau(m/d) \tau(n/d). \tag{6}
\]

Proof. The number of all subgroups is the cardinality of the set \( J_{m,n} \), that is

\[
s(m, n) = \sum_{a \mid m} \sum_{b \mid a} \sum_{c \mid n} \sum_{d \mid c} \phi(e). \tag{7}
\]

Let \( m = ax, \; a = by, \; n = cz, \; c = dt \). Then, by the condition \( a/b = c/d = e \) we have \( y = t = e \). Rearranging the terms,

\[
s(m, n) = \sum_{i \mid m} \sum_{j \mid n} \phi(e) = \sum_{i \mid m} \sum_{j \mid n} \phi(ij/\delta) \tau(m/\delta) \tau(n/\delta),
\]

finishing the proof of (5). To obtain the formula (6) write (7) as follows:

\[
s(m, n) = \sum_{e \mid \gcd(m,n)} \phi(e) \sum_{k \mid m} \sum_{\ell \mid n} 1 = \sum_{e \mid \gcd(m,n)} \phi(e) \tau(m/e) \tau(n/e).
\]

Note that (5) is a special case of an identity deduced in [3] by different arguments. Now consider \( s_{\delta}(m, n) \), denoting the number of subgroups of order \( \delta \) of \( \mathbb{Z}_m \times \mathbb{Z}_n \).

Proposition 4.2. For every \( m, n, \delta \in \mathbb{N} \) such that \( \delta \mid mn \),

\[
s_{\delta}(m, n) = \sum_{ij \mid \gcd(m,\delta) \delta \mid \gcd(n,\delta)} \phi\left(\frac{ij}{\delta}\right). \tag{8}
\]

Proof. Similar to the proof of above. We have

\[
s_{\delta}(m, n) = \sum_{a \mid m} \sum_{c \mid n} \sum_{\substack{a/b = c/d = \delta \mid \delta \mid \gcd(m,\delta) \delta \mid \gcd(n,\delta) \delta \mid \delta}} \phi(e)
\]

\[
= \sum_{\substack{b \mid m \; d \mid n \; bde = \delta \mid \delta \mid \gcd(m,\delta) \delta \mid \gcd(n,\delta) \delta \mid \delta}} \phi(e),
\]

where the only term of the inner sum is obtained for \( e = ij/\delta \) provided that \( \delta \mid ij, \; i \mid \delta \) and \( j \mid \delta \). This gives (8).
The number of subgroups with a given type of \( \mathbb{Z}_m \times \mathbb{Z}_n \) is given by the following formula.

**Proposition 4.3.** Let \( m, n \in \mathbb{N} \) and let \( A, B \in \mathbb{N} \) such that \( A \mid B \). Let \( A \mid \gcd(m, n) \). Then the number \( N_{A,B}(m, n) \) of subgroups of \( \mathbb{Z}_m \times \mathbb{Z}_n \), which are isomorphic to \( \mathbb{Z}_A \times \mathbb{Z}_B \), is given by

\[
N_{A,B}(m, n) = \sum_{i | m, j | n \atop AB | ij, \text{lcm}(i,j)=B} \phi \left( \frac{ij}{AB} \right).
\]

(9)

If \( A \nmid \gcd(m, n) \), then \( N_{A,B}(m, n) = 0 \).

**Proof.** Using Proposition 3.1/ ii) we have

\[
N_{A,B}(m, n) = \sum_{a | m \atop b | a} \sum_{c | n \atop d | c} \sum_{e | m \atop f | e} \sum_{g | n \atop h | g} \phi(e).
\]

Here the condition \( \gcd(b, d) = A \) implies that \( A \mid m \) and \( A \mid n \). In this case

\[
N_{A,B}(m, n) = \sum_{i | m \atop j | n} \sum_{\gcd(i, j)=\delta} \phi(e),
\]

where the only term of the inner sum is obtained for \( e = ij/(AB) \) provided that \( AB \mid ij \), \( i \mid AB \) and \( j \mid AB \).

From the representation of the cyclic subgroups given in Proposition 3.1/ iv) we also deduce the next result.

**Proposition 4.4.** For every \( m, n \in \mathbb{N} \) the number \( c(m, n) \) of cyclic subgroups of \( \mathbb{Z}_m \times \mathbb{Z}_n \) is

\[
c(m, n) = \sum_{i | m, j | n \atop \gcd(i, j)=\delta} \phi(\gcd(i, j))
\]

(10)

\[
= \sum_{d \mid \gcd(m,n)} (\mu * \phi)(d)\tau(m/d)\tau(n/d).
\]

(11)

**Proof.** Similar to the proofs of above, using that for the cyclic subgroups one has \( \gcd(b, d) = 1 \).

Let \( c_{\delta}(m, n) \) denote the number of cyclic subgroups of order \( \delta \) of \( \mathbb{Z}_m \times \mathbb{Z}_n \).

**Proposition 4.5.** For every \( m, n, \delta \in \mathbb{N} \) such that \( \delta \mid mn \),

\[
c_{\delta}(m, n) = \sum_{i | m, j | n \atop \text{lcm}(i,j)=\delta} \phi(\gcd(i, j)).
\]

**Proof.** This is a direct consequence of (9) obtained in the case \( A = 1 \) and \( B = \delta \).

In the paper \([7]\) the identities (5), (6), (8), (10) and (11) were derived using another approach. The identity (10), as a special case of a formula valid for arbitrary finite Abelian groups, was obtained by the author \([16, 17]\) using different arguments. Finally, we remark that the functions \((m, n) \mapsto s(m, n)\) and \((m, n) \mapsto c(m, n)\) are multiplicative, viewed as arithmetic functions of two variables. See \([7, 18]\) for details.
5 Table of the subgroups of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

To illustrate our results we describe the subgroups of the group $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ ($m = 12, n = 18$). According to Proposition 4.3, there exist subgroups isomorphic to $\mathbb{Z}_A \times \mathbb{Z}_B$ ($A \mid B$) if and only if $A \mid \gcd(12, 18) = 6$, that is $A \in \{1, 2, 3, 6\}$.

| Number subgroups | 80 |
|------------------|----|
| Number subgroups order 1 | 1 |
| Number subgroups order 2 | 3 |
| Number subgroups order 3 | 4 |
| Number subgroups order 4 | 3 |
| Number subgroups order 6 | 12 |
| Number subgroups order 8 | 1 |
| Number subgroups order 9 | 4 |
| Number subgroups order 12 | 12 |
| Number cyclic subgroups | 48 |
| Number noncyclic subgroups | 32 |
| Number subgroups $\simeq \mathbb{Z}_1$ | 1 |
| Number subgroups $\simeq \mathbb{Z}_2$ | 3 |
| Number subgroups $\simeq \mathbb{Z}_3$ | 4 |
| Number subgroups $\simeq \mathbb{Z}_4$ | 2 |
| Number subgroups $\simeq \mathbb{Z}_6$ | 12 |
| Number subgroups $\simeq \mathbb{Z}_9$ | 3 |
| Number subgroups $\simeq \mathbb{Z}_{12}$ | 8 |
| Number subgroups $\simeq \mathbb{Z}_{18}$ | 9 |
| Number subgroups $\simeq \mathbb{Z}_{36}$ | 6 |

Table of the subgroups of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

6 Acknowledgement

The author gratefully acknowledges support from the Austrian Science Fund (FWF) under the project Nr. M1376-N18. The author thanks D. D. Anderson and J. Petrillo for sending him copies of their papers quoted in the References.
References

[1] D. D. Anderson, V. Camillo, Subgroups of direct products of groups, ideals and subrings of direct products of rings, and Goursat’s lemma. Rings, modules and representations, *Contemp. Math.*, vol. 480, Amer. Math. Soc., Providence, RI, 2009, pp. 1–12.

[2] K. Bauer, D. Sen, P. Zvengrowski, A generalized Goursat lemma, Preprint, 2011, arXiv:11009.0024 [math.GR].

[3] W. C. Calhoun, Counting the subgroups of some finite groups, *Amer. Math. Monthly* **94** (1987), 54–59.

[4] G. Călugăreanu, The total number of subgroups of a finite abelian group, *Sci. Math. Jpn.* **60** (2004), 157–167.

[5] R. R. Crawford, K. D. Wallace, On the number of subgroups of index two — An application of Goursat’s theorem for groups, *Math. Mag.* **48** (1975), 172–174.

[6] É. Goursat, Sur les substitutions orthogonales et les divisions régulières de l’espace, *Ann. Sci. École Norm. Sup.* (3) **6** (1889), 9–102.

[7] M. Hampejs, N. Holighaus, L. Tóth, C. Wiesmeyr, Representing and counting the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$, *Journal of Numbers*, accepted, arXiv:1211.1797 [math.GR].

[8] M. Hampejs, L. Tóth, On the subgroups of finite Abelian groups of rank three, *Annales Univ. Sci. Budapest., Sect Comp.* **39** (2013), 111–124.

[9] J. Lambek, Goursat’s theorem and the Zassenhaus lemma, *Canad. J. Math.* **10** (1958), 45–56.

[10] A. Machi, *Groups. An Introduction to Ideas and Methods of the Theory of Groups*, Springer, 2012.

[11] W. G. Nowak, L. Tóth, On the average number of subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$, *Int. J. Number Theory* **10** (2014), 363–374, arXiv:1307.1414 [math.NT].

[12] J. Petrillo, Goursat’s other theorem, *College Math. J.* **40** (2009), 119–124.

[13] J. Petrillo, Counting subgroups in a direct product of finite cyclic groups, *College Math. J.* **42** (2011), 215–222.

[14] J. J. Rotman, *An Introduction to the Theory of Groups*, Fourth Ed., Springer, 1995.

[15] M. Tărnăuceanu, An arithmetic method of counting the subgroups of a finite abelian group, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **53(101)** (2010), 373–386.

[16] L. Tóth, Menon’s identity and arithmetical sums representing functions of several variables, *Rend. Sem. Mat. Univ. Politec. Torino* **69** (2011), 97–110.

[17] L. Tóth, On the number of cyclic subgroups of a finite Abelian group, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **55(103)** (2012), 423–428.
[18] L. Tóth, Multiplicative arithmetic functions of several variables: a survey, in *Mathematics Without Boundaries, Surveys in Pure Mathematics*, Th. M. Rassias, P. Pardalos (Eds.), Springer, 2014, 483–514, arXiv:1310.7053 [math.NT].

L. Tóth
Institute of Mathematics, Universität für Bodenkultur
Gregor Mendel-Straße 33, A-1180 Vienna, Austria
and
Department of Mathematics, University of Pécs
Ifjúság u. 6, H-7624 Pécs, Hungary
E-mail: ltoth@gamma.ttk.pte.hu