When is a subgroup of a ring an ideal?

Sunil K. Chebolu and Christina L. Henry
When is a subgroup of a ring an ideal?

Sunil K. Chebolu and Christina L. Henry

(Communicated by Kenneth S. Berenhaut)

Let $R$ be a commutative ring. When is a subgroup of $(R, +)$ an ideal of $R$? We investigate this problem for the rings $\mathbb{Z}^d$ and $\prod_{i=1}^{d} \mathbb{Z}/n_i \mathbb{Z}$. In the cases of $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}/n \times \mathbb{Z}/m$, our results give, for any given subgroup of these rings, a computable criterion for the problem under consideration. We also compute the probability that a randomly chosen subgroup from $\mathbb{Z}/n \times \mathbb{Z}/m$ is an ideal.

1. Introduction

Let $R$ be a commutative ring. The object of this paper is to determine necessary and sufficient conditions for a given subgroup of $(R, +)$ to be an ideal of $R$. Our motivation for asking this question arose from some problems on Mathieu subspaces (more is explained in the next paragraph). To begin, consider the ring $\mathbb{Z}$ of integers. Every subgroup of $\mathbb{Z}$ is of the form $k \mathbb{Z}$ for some integer $k$, and each of these subgroups is clearly also an ideal. In fact, the same is true also for the ring $\mathbb{Z}/n$ (the ring of integers modulo $n$). It turns out that these are the only rings $R$ in which every subgroup of $(R, +)$ is also an ideal of $R$; see Proposition 2.1. In particular, when we consider product rings, we get some subgroups that are not ideals. For instance, the diagonal $\{(x, x) \mid x \in \mathbb{Z}\}$ in $\mathbb{Z} \times \mathbb{Z}$ is clearly a subgroup of $(\mathbb{Z} \times \mathbb{Z}, +)$ but not an ideal in the ring $\mathbb{Z} \times \mathbb{Z}$. In this paper, we consider the product rings $\mathbb{Z}^d$ (in Section 3) and $\prod_{i=1}^{d} \mathbb{Z}/n_i \mathbb{Z}$ (in Section 4), and for various subgroups of these rings, we give necessary and sufficient conditions for a given subgroup to be an ideal. In the cases of $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}/n \times \mathbb{Z}/m$, our necessary and sufficient conditions are also computable for any given subgroup of these rings. As one would expect, our results show that in general an arbitrary subgroup of a ring is seldom an ideal. In fact, we make this statement precise in Theorem 5.4, where we compute explicitly the probability that a randomly chosen subgroup from $\mathbb{Z}/n \times \mathbb{Z}/m$ is an ideal. For instance, when $p$ is a prime and the ring is $\mathbb{Z}/p \times \mathbb{Z}/p$, this probability is only $4/(p + 3)$. We will use several basic facts and tools from abstract algebra, which can be found in

MSC2010: primary 13AXX; secondary 20KXX.

Keywords: ring, subgroup, ideal, Mathieu subspace, Goursat.

Chebolu is supported by an NSA grant (H98230-13-1-0238).
We also use a theorem in group theory due to Goursat; a good exposition of this theorem can be found in [Petrillo 2011], and we review it in Theorem 4.4. Although we focus mainly on the rings $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$, where possible we offer some generalizations. By a subgroup of a ring $R$, we always mean a subgroup of the additive group $(R, +)$.

This problem came up naturally when Chebolu and his collaborators (Yamskulna and Zhao) were recently working on some problems involving Mathieu subspaces in some rings. A Mathieu subspace is a generalization of an ideal: for a commutative ring $R$, a $\mathbb{Z}$-submodule $M$ of $R$ is said to be a Mathieu subspace of $R$ if whenever $a^n$ belongs to $M$ (for all $n \geq 1$), then $ra^n$ belongs to $M$ for all $n$ sufficiently large. Every ideal is a Mathieu subspace, but the converse is not necessarily true. The notion of a Mathieu subspace was introduced by Wenhua Zhao [2010], and it proved to be a central idea in the research on several landmark conjectures in algebra and geometry, including the Jacobian conjecture. As a result, Mathieu subspaces received serious attention and extensive writing; see [Zhao 2012] and the references therein. Chebolu and his collaborators were led to the problem of determining when a subgroup of a ring is a Mathieu subspace. Since ideals are important and relatively well-understood classes of Mathieu subspaces, it was natural to investigate the same question for ideals. Thus the problem we study in this paper is an interesting offshoot of our Mathieu subspaces project.

2. Generators

In the introduction, we noted that the rings $\mathbb{Z}$ and $\mathbb{Z}_n$ have the property that every subgroup in them is also an ideal. It is not hard to show that these are the only rings with this property.

**Proposition 2.1.** Let $R$ be a unital commutative ring, i.e., a commutative ring with a multiplicative identity. If every subgroup of $(R, +)$ is also an ideal, then $R$ is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$ for some positive integer $n$.

**Proof.** Since $R$ is a unital ring, there is a natural map $\phi: \mathbb{Z} \to R$ that sends 1 to $1_R$, the multiplicative identity of $R$. The image of this homomorphism is exactly the subgroup of $(R, +)$ that is generated by $1_R$. If every subgroup of $(R, +)$ is an ideal, then, in particular, the subgroup generated by $1_R$ is also an ideal. However, the only ideal that contains $1_R$ is the entire ring $R$. This means $\phi$ is surjective. From the first isomorphism theorem, we have $\mathbb{Z} / \ker \phi \cong R$. It follows that $R$ is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some integer $n$. (In the former case, $R$ has characteristic 0, and in the latter, $R$ has characteristic $n$.) \qed

We will now show that every subgroup of $\mathbb{Z}^d$ or $\prod_{i=1}^d \mathbb{Z}_{n_i}$ is generated by at most $d$ elements. We will recall some standard results from abstract algebra, which can be found in [Dummit and Foote 2004].
Theorem 2.2. Let \( R \) be a PID and let \( M \) be a free \( R \)-module of rank \( r \). Then every submodule of \( M \) is also free and has rank at most \( r \).

This theorem takes care of \( \mathbb{Z}^d \). For \( \prod_{i=1}^d \mathbb{Z}_{n_i} \), we need the following corollary, which can be derived easily from the above theorem.

Corollary 2.3. Let \( R \) be a PID and let \( M \) be a finitely generated \( R \)-module. If \( M \) is generated by \( r \) elements, then every submodule of \( M \) is generated by at most \( r \) elements.

Corollary 2.4. Every subgroup of \( \left( \prod_{i=1}^d \mathbb{Z}_{n_i}, + \right) \) or of \( (\mathbb{Z}^d, +) \) is generated by at most \( d \) elements.

Proof. The ring \( \prod_{i=1}^d \mathbb{Z}_{n_i} \) is a \( \mathbb{Z} \)-module that is clearly generated by \( d \) elements; the standard basis forms a generating set. Therefore by the above corollary, every subgroup of \( \prod_{i=1}^d \mathbb{Z}_{n_i} \) is generated by at most \( d \) elements. The corresponding statement for \( \mathbb{Z}^d \) is a special case of the above theorem.

This corollary gives a natural stratification of the class of all nonsubgroups of these rings, which is based on the minimal number of generators of a given subgroup. This stratification will be helpful in our analysis.

3. The ring \( \mathbb{Z} \times \mathbb{Z} \)

In this section, we determine when a given additive subgroup of the ring \( \mathbb{Z}^d \) is an ideal. The trivial subgroup, which consists of the single element \( (0, 0, \ldots, 0) \), is also trivially an ideal, so we will consider nonzero subgroups. As explained in the previous section, a nonzero subgroup of \( \mathbb{Z}^d \) is free of rank at most \( d \). We will begin with rank-1 subgroups, where the problem is straightforward.

Proposition 3.1. Let \( L \) be a subgroup of \( \mathbb{Z}^d \) generated by \( (a_1, \ldots, a_d) \). Then \( L \) is an ideal if and only if all but one of the \( a_i \) are zero.

Proof. If all but one of the \( a_i \) are zero, then \( L \) is clearly an ideal in one of the factors of \( \mathbb{Z}^d \). On the other hand, if we have more than one nonzero \( a_i \), say \( a_i \) and \( a_j \), then consider \( e_i = (0, \ldots, 0, 1, 0 \ldots, 0) \), which has 1 at the \( i \)-th spot. If \( L \) is an ideal, then \( e_i(a_1, \ldots, a_d) = (0, \ldots, 0, a_i, 0, \ldots, 0) \) should belong to \( L \). This is a contradiction, so we are done.

More generally, the following is true.

Lemma 3.2. Let \( R \) be an integral domain. A subgroup of \( (R, +) \) generated by a nonzero element \( a \) is an ideal of \( R \) if and only if \( R \) is isomorphic to \( \mathbb{Z} \) or \( \mathbb{Z}_p \) for some prime \( p \).

Proof. Let \( \langle a \rangle \) be the additive subgroup of \( (R, +) \) generated by \( a \) (\( \neq 0 \)). Let \( r \) be an arbitrary element of \( R \). If \( \langle a \rangle \) is an ideal, then we should have \( ra = na \) for some integer \( n \). This equation implies that \( (r-n1_R)a = 0 \). Since we are working in an integral
domain and $a$ is nonzero, we get $r - n1_R = 0$, or $r = n1_R$. Since $r$ is arbitrary, this implies that $(R, +)$ is a cyclic group generated by $1_R$. This means $R$ is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n$. But since $R$ is an integral domain, $n$ has to be a prime. 

Now we move on to subgroups of rank at least $2$ in $\mathbb{Z}^d$, where the problem is more interesting. We begin with an example to show the subtlety in the problem.

**Example 3.3.** Consider the ring $\mathbb{Z} \times \mathbb{Z}$ and let $S$ and $T$ denote the following rank-2 subgroups of $(\mathbb{Z} \times \mathbb{Z}, +)$:

$$S = \{(2, 0), (3, 1)\},$$

$$T = \{(2, 0), (2, 1)\}.$$

We claim that $S$ is not an ideal but $T$ is. If $S$ is an ideal, then the element $(0, 1)$ should belong to it. That means the pair of equations $2x + 3y = 0$ and $y = 1$ have to be consistent over $\mathbb{Z}$. However, it is easy to see that this is not the case. On the other hand, $T$ is an ideal in $\mathbb{Z} \times \mathbb{Z}$. In fact, $T = 2\mathbb{Z} \times \mathbb{Z}$. See Theorem 3.8 for the general result.

We begin by classifying ideals of $\mathbb{Z}^d$ whose additive groups are free of rank $k$.

**Proposition 3.4.** Let $I$ be an ideal in $\mathbb{Z}^d$. Then $I$ is free of rank $k$ $(1 \leq k \leq n)$ if and only if $I$ is of the form $\prod_{i=1}^{d} d_i \mathbb{Z}$, where exactly $k$ of the numbers $d_i$ are nonzero.

**Proof.** Recall that every ideal in $\mathbb{Z}^d$ is of the form $\prod_{i=1}^{d} d_i \mathbb{Z}$, where the $d_i$ are integers. The rank of $\prod_{i=1}^{d} d_i \mathbb{Z}$ is exactly the number of $d_i$ that are nonzero. 

In view of this proposition, to determine when a subgroup of rank $k$ in $\mathbb{Z}^d$ is an ideal, it is enough (after deleting the zero coordinates) to consider the problem when $d = k$. The latter is addressed in the next two theorems. We begin with a lemma that we will need in these theorems. Recall that an integer matrix $A$ is said to be unimodular if it is invertible over the ring of integers. This statement is equivalent (as can be seen by Cramer’s formula for the inverse) to saying that the determinant of $A$ is either 1 or $-1$. In the following lemma, a subgroup of $\mathbb{Z}^n$ of rank $n$ will be called a lattice of $\mathbb{Z}^n$.

**Lemma 3.5.** Let $A$ and $B$ be two $n \times n$ matrices over the integers that are invertible over the rationals. The columns of $A$ and those of $B$ form two bases for a lattice $L$ if and only if there exists a unimodular matrix $X$ such that $AX = B$.

**Proof.** Since the columns of $A$ and $B$ form a basis for $L$, there exist integer square matrices $X$ and $Y$ such that $AX = B$ and $BY = A$. Multiplying the first equation on the right-hand side by $Y$, we get $AXY = BY$. But $BY = A$, so we get $AXY = A$. Since $A$ is invertible over the rationals, we multiply the inverse (over the rationals) of $A$ on both sides to conclude that $XY = I$. This means $X$ is invertible over $\mathbb{Z}$ (i.e., it is unimodular) and $AX = B$. For the other direction, let $Y$ be the inverse
of $X$ over $\mathbb{Z}$, so we have $AX = B$ and $BY = A$. The first equation tells us that the column space of $B$ is contained in that of $A$, and the second equation says that the column space of $A$ is contained in that of $B$. □

**Theorem 3.6.** Let $H$ be a subgroup of rank $k$ in $\mathbb{Z}^k$. Let the columns of a $k \times k$ matrix $A$ be a $\mathbb{Z}$-basis for $H$. Then the following are equivalent:

1. $H$ is an ideal in $\mathbb{Z}^k$.
2. There exists a unimodular matrix $U$ such that $AU$ is a diagonal matrix.
3. There is a sequence of elementary row operations (over $\mathbb{Z}$) that can convert $A$ into a diagonal matrix.

**Proof.** Let $H$ (as in the statement of the theorem) be an ideal in $\mathbb{Z}^k$. Then by Proposition 3.4, $H$ is of the form $\prod_{i=1}^{k} d_i \mathbb{Z}$ for some integers $d_i$. Since $H$ has rank $k$, all these integers have to be nonzero. $H$ can be written in this form if and only if the columns of $A$ and those of the diagonal matrix $D = \text{Diagonal}(d_1, \ldots, d_k)$ form a basis for $H$. By the above lemma, this happens if and only if there is a unimodular matrix $U$ such that $AU = D$. Hence we have the equivalence of statements (1) and (2). The equivalence of (2) and (3) for the field of real numbers is well-known (the famous reduced row echelon form of an invertible matrix). The reader can verify that the proof works over $\mathbb{Z}$ when properly interpreted. For instance, the role played by nonzero real numbers in the world of $\mathbb{Z}$ are the units $\pm 1$. This gives the equivalence of statements (2) and (3). □

Since $\mathbb{Z}$ is a Euclidean domain where we can talk about gcds, we can take the above theorem one step further. Let $A^*$ denote the adjoint matrix of $A$. Recall that the formula for the inverse of $A$ (an invertible matrix) is given by

$$A^{-1} = \frac{1}{\det(A)} A^* = \frac{1}{\det(A)} ((a_{ij}^*)) .$$

**Theorem 3.7.** Let $H$ be a subgroup of rank $k$ in $\mathbb{Z}^k$. Let the columns of a $k \times k$ matrix $A$ be a $\mathbb{Z}$-basis for $H$. Then the following are equivalent:

1. $H$ is an ideal in $\mathbb{Z}^k$.
2. There exists a unimodular matrix $U$ such that $AU$ is a diagonal matrix.
3. There is a sequence of $k$ nonzero integers $d_1, d_2, \ldots, d_k$ such that
   
   (a) $\det(A) = \pm d_1 d_2 \cdots d_k$,
   
   (b) $\det(A)/d_i$ divides $\gcd(a_{1i}^*, \ldots, a_{ki}^*)$ for all $i$.

**Proof.** We already saw the equivalence of (1) and (2) in Theorem 3.6. Now we will show that (2) and (3) are equivalent. Let $H$ and $A$ be as in the statement of the theorem. There exists a unimodular matrix $U$ such that $AU$ is a diagonal matrix if
and only if for some diagonal matrix $D = \text{Diagonal}(d_1, \ldots, d_k)$, the matrix $A^{-1}D$ is unimodular. Using Cramer’s formula for the inverse, we can equivalently say that

$$X = \frac{1}{\det(A)} A^* D$$

is unimodular. Since $X$ is unimodular, its determinant is $\pm 1$. Taking determinants of both sides of the above matrix equation will give (a). Moreover, the entries of $X$ should be all integers. For that to happen, $\det(A)$ should divide all the entries in each of the columns $a_{1i}, \ldots, a_{ki}$.

We can tell exactly when condition (2) of Theorem 3.7 holds in the case of $\mathbb{Z} \times \mathbb{Z}$. That gives the following result, which along with the rank-1 result proved earlier, gives a full answer to our problem for the ring $\mathbb{Z} \times \mathbb{Z}$.

**Theorem 3.8.** Let $L$ be a rank-2 subgroup of $\mathbb{Z} \times \mathbb{Z}$ that is generated by vectors $(a, b)$ and $(c, d)$. Then $L$ is an ideal in $\mathbb{Z} \times \mathbb{Z}$ if and only if $ad - bc$ divides $\gcd(a, c) \gcd(b, d)$.

**Proof.** Let $L$ be a rank-2 subgroup of $\mathbb{Z} \times \mathbb{Z}$ that is generated by vectors $(a, b)$ and $(c, d)$, and let $A$ be the $2 \times 2$ matrix with these two columns. From the above theorems, and using the formula for the inverse of a $2 \times 2$ matrix, we conclude that $L$ is an ideal if and only if there exist nonzero integers $d_1$ and $d_2$ such that

1. $ad - bc = \pm d_1 d_2$,
2. $(ad - bc)/d_1$ divides $\gcd(b, d)$ and $(ad - bc)/d_2$ divides $\gcd(a, c)$.

We claim that nonzero integers $d_1$ and $d_2$ exist with these properties if and only if $ad - bc$ divides $\gcd(a, c) \gcd(b, d)$. If $d_1$ and $d_2$ exist such that (1) and (2) hold, then from (2) we get $(ad - bc)^2/(d_1 d_2)$ divides $\gcd(a, c) \gcd(b, d)$, but $(ad - bc)^2/(d_1 d_2) = ad - bc$. This proves one direction. For the other, direction, suppose $ad - bc$ divides $\gcd(a, c) \gcd(b, d)$. Then an elementary number theory fact tells us we can write $ad - bc$ as $d_1 d_2$, where $d_1$ divides $\gcd(a, c)$ and $d_2$ divides $\gcd(b, d)$.

We now explain how one can arrive at Theorem 3.8 more directly by solving linear equations over $\mathbb{Z}$. Recall that our problem boils down to the following question. **Given an integer matrix $A$ with nonzero determinant, when does there exist a unimodular matrix $X$ such that $AX$ is a diagonal matrix?** To address this, we let $X = (x_{ij})$ and consider the matrix equation

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}.$$
This gives us the set of equations
\[\begin{align*}
ax_{12} + cx_{22} &= 0, \quad (3-1) \\
bx_{11} + dx_{21} &= 0, \quad (3-2) \\
x_{11}x_{22} - x_{12}x_{21} &= 1. \quad (3-3)
\end{align*}\]

(\(X\) is unimodular, so its determinant is either 1 or \(-1\). However, by swapping the columns of \(A\) if necessary, we may assume that the determinant of \(X\) is 1, which gives us the third equation.) \(L\) is an ideal if and only if the above system of equations has a solution in integers \(x_{ij}\). Let us begin with (3-1): \(ax_{12} + cx_{22} = 0\) if and only if \(ax_{12} = -cx_{22}\). Then
\[x_{12} = \frac{-c}{\gcd(a,c)} \alpha, \quad x_{22} = \frac{a}{\gcd(a,c)} \alpha \quad \text{for some integer } \alpha.\]

Similarly, using (3-2), we get
\[x_{11} = \frac{-d}{\gcd(b,d)} \beta, \quad x_{21} = \frac{b}{\gcd(b,d)} \beta \quad \text{for some integer } \beta.\]

Substituting these values in the determinant condition (3-3), we get
\[1 = x_{11}x_{22} - x_{12}x_{21} = \frac{-d}{\gcd(b,d)} \frac{b}{\gcd(b,d)} \frac{-c}{\gcd(a,c)} \alpha - \frac{-c}{\gcd(a,c)} \frac{b}{\gcd(b,d)} \beta = \frac{-ad}{\gcd(a,c) \gcd(b,d)} - \frac{-bc}{\gcd(a,c) \gcd(b,d)}.\]

Hence,
\[\gcd(a,c) \gcd(b,d) = -\alpha \beta (ad - bc). \quad (3-4)\]

Thus we see from (3-4) that the set of equations (3-1)–(3-3) is consistent over \(\mathbb{Z}\) if and only if \(\det(A) = ad - bc\) divides \(\gcd(a,c) \gcd(b,d)\) in \(\mathbb{Z}\). In that case, we can take \(\alpha = -1\) and \(\beta = \frac{\gcd(a,c) \gcd(b,d)}{ad - bc}\).

This completes the alternative proof of Theorem 3.8.

The following corollary follows immediately from Theorem 3.8.

**Corollary 3.9.** Let \((a, b)\) and \((c, d)\) be two vectors in \(\mathbb{Z} \times \mathbb{Z}\) and \(L\) be the lattice generated by these two vectors.

1. If \(ad - bc = \pm 1\), then \(L\) is an ideal in \(\mathbb{Z} \times \mathbb{Z}\).
2. If \(ad - bc\) is a prime, then \(L\) is an ideal if and only if \(ad - bc\) divides either \(\gcd(a,c)\) or \(\gcd(b,d)\).
4. The ring $\mathbb{Z}_n \times \mathbb{Z}_m$

Let $n$ and $m$ be positive integers and consider the ring $\mathbb{Z}_n \times \mathbb{Z}_m$. Our problem is to determine when a subgroup of $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$ is an ideal. We have seen that a nonzero subgroup of $\mathbb{Z}_n \times \mathbb{Z}_m$ is generated by either one or two elements, so we have two cases to consider. First, consider a subgroup $L$ in the ring $\mathbb{Z}_n \times \mathbb{Z}_m$ that is generated by $(a, b)$. If either $a = 0$ in $\mathbb{Z}_n$ or $b = 0$ in $\mathbb{Z}_m$, the problem is trivial because $L$ is simply an ideal in one of the components of $\mathbb{Z}_n \times \mathbb{Z}_m$. So let us assume that both $a$ and $b$ are nonzero in their respective component rings. Then we have the following theorem.

**Theorem 4.1.** Let $1 \leq a < n$ and $1 \leq b < m$. The subgroup generated by $(a, b)$ in the ring $\mathbb{Z}_n \times \mathbb{Z}_m$ is an ideal if and only if $\gcd\left(\frac{n}{\gcd(a, n)}, \frac{m}{\gcd(b, m)}\right) = 1$.

**Proof.** Since our rings are principal ideal rings, every ideal in $\mathbb{Z}_n \times \mathbb{Z}_m$ is of the form $d_1 \mathbb{Z}_n \times d_2 \mathbb{Z}_m$, where $d_1$ and $d_2$ are some integers. For brevity, we will denote this ideal by $\langle d_1 \rangle \times \langle d_2 \rangle$.

Returning to our problem, let us assume that the line $L$ generated by $(a, b)$ is an ideal of $\mathbb{Z}_n \times \mathbb{Z}_m$. From above, we have
\[ L = \langle d_1 \rangle \times \langle d_2 \rangle. \]

Consider the restrictions to $L$ of the natural projection maps: $\pi_1 : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_n$ and $\pi_2 : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_m$. We will compute $\pi_1(L)$ in two different ways. On the one hand, since $L = \langle d_1 \rangle \times \langle d_2 \rangle$, we have $\pi_1(L) = \langle d_1 \rangle$. On the other hand, $L$ is generated by $(a, b)$, so the first components of the elements of $L$ pick up all multiples of $a$. Therefore $\pi_1(L) = \langle a \rangle$. This shows that $\langle a \rangle = \langle d_1 \rangle$. Similarly, working with the second projection map, we conclude that $\langle b \rangle = \langle d_2 \rangle$.

To summarize, $L$ spanned by $(a, b)$ is an ideal if and only if
\[ \langle (a, b) \rangle = \langle a \rangle \times \langle b \rangle. \]

The inclusion $\langle (a, b) \rangle \subseteq \langle a \rangle \times \langle b \rangle$ is obvious. Therefore, equality holds if and only if both sides have the same cardinality. These cardinalities are given by the following formulas (ord $x$ denotes the additive order of $x$):
\[ |\langle (a, b) \rangle| = \text{lcm}(\text{ord } a, \text{ord } b) = \frac{\text{ord } a \text{ ord } b}{\gcd(\text{ord } a, \text{ord } b)}, \]
\[ |\langle a \rangle \times \langle b \rangle| = \text{ord } a \text{ ord } b. \]

Equating these two expressions, clearly $L$ spanned by $(a, b)$ in $\mathbb{Z}_n \times \mathbb{Z}_m$ is an ideal if and only $\gcd(\text{ord } a, \text{ord } b) = 1$. The theorem now follows from the fact that the order of an element $c$ in $(\mathbb{Z}_s, +)$ is given by $s/\gcd(c, s)$. $\square$
Remark 4.2. When $m$ and $n$ are relatively prime, Theorem 4.1 implies that every line in $\mathbb{Z}_n \times \mathbb{Z}_m$ is an ideal. This is indeed the case because for relatively prime integers $m$ and $n$, we have $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

More generally, the following theorem is true:

**Theorem 4.3.** The subgroup generated by the element $(a_1, a_2, \ldots, a_k)$ in the ring $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is an ideal if and only if

$$\prod_{1 \leq i < j \leq n} \gcd\left(\frac{n_j}{\gcd(a_i, n_i)}, \frac{n_j}{\gcd(a_j, n_j)}\right) = 1.$$

**Proof.** From the proof of Theorem 4.1, it follows that the subgroup generated by the element $(a_1, a_2, \ldots, a_k)$ in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is an ideal if and only if

$$\prod_i \operatorname{ord} a_i = \operatorname{lcm} \operatorname{ord} a_i.$$

Showing that this last equation holds if and only if

$$\prod_{1 \leq i < j \leq n} \gcd(\operatorname{ord} a_i, \operatorname{ord} a_j) = 1$$

can be done as an exercise. Then using the formula mentioned above for the order of an element in $\mathbb{Z}_s$, we now get the condition given in the statement of the theorem. □

We now investigate when a subgroup of $\mathbb{Z}_n \times \mathbb{Z}_m$ generated by two elements is an ideal. To this end, the following theorem from group theory, due to Goursat, will be useful. We will also use this theorem in the next section, where we compute some probabilities.

**Theorem 4.4** (Goursat [Petrillo 2011]). Let $G_1$ and $G_2$ be any two groups. There exists a bijection between the set $S$ of all subgroups of $G_1 \times G_2$ and the set $T$ of all 5-tuples $(A_1, B_1, A_2, B_2, \phi)$, where $A_i$ is a subgroup of $G_i$, $B_i$ is a normal subgroup of $A_i$, and $\phi$ is a group isomorphism from $A_1/B_1$ to $A_2/B_2$.

Let $\pi_i: G_1 \times G_2 \to G_i$ denote the projection homomorphisms. The desired bijection in this theorem is given as follows. For a subgroup $U$ of $G_1 \times G_2$, we define a 5-tuple $(A_{U_1}, B_{U_1}, A_{U_2}, B_{U_2}, \phi_U)$, where

$$A_{U_1} = \operatorname{Im}(\pi_1|_U),$$

$$B_{U_1} = \pi_1(\ker(\pi_2|_U)),$$

$$A_{U_2} = \operatorname{Im}(\pi_2|_U),$$

$$B_{U_2} = \pi_2(\ker(\pi_1|_U)),$$

$$\phi_U(a_1 B_{U_1}) = a_2 B_{U_2}, \quad \text{when } (a_1, a_2) \in U.$$
Conversely, given a 5-tuple \((A_1, B_1, A_2, B_2, \phi)\), the corresponding subgroup \(U\) of \(G_1 \times G_2\) is given by

\[
U_\phi = \{(a_1, a_2) \in A_1 \times A_2 \mid \phi(a_1 B_1) = a_2 B_2\}.
\]

**Corollary 4.5.** Let \(G_1 \times G_2\) be a finite group and let \((A_{U_1}, B_{U_1}, A_{U_2}, B_{U_2}, \phi_U)\) correspond to the subgroup \(U\) of \(G_1 \times G_2\). Then we have

\[
|U| = |A_{U_1}| |B_{U_2}|.
\]

**Proof.** It is clear from the correspondence in Goursat’s theorem that

\[
|U| = |A_{U_1} / B_{U_1}| |B_{U_1} / B_{U_2}| = |A_{U_1}| |B_{U_2}|.
\]

Given elements \(\alpha\) and \(\beta\) in \(\mathbb{Z}_n\), consider the linear map \(\phi_{\alpha, \beta}: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n\) defined by \(\phi_{\alpha, \beta}(x, y) = \alpha x + \beta y\). Then we have the following theorem.

**Theorem 4.6.** The subgroup of \(\mathbb{Z}_n \times \mathbb{Z}_m\) generated by \((a, b)\) and \((c, d)\) is an ideal of \(\mathbb{Z}_n \times \mathbb{Z}_m\) if and only if

\[
(\ker \phi_{a, c})(\ker \phi_{b, d}) = \mathbb{Z} \times \mathbb{Z}.
\]

**Proof.** Let \(H\) denote the subgroup generated by \((a, b)\) and \((c, d)\) in \(\mathbb{Z}_n \times \mathbb{Z}_m\). Suppose \(H\) is an ideal in \(\mathbb{Z}_n \times \mathbb{Z}_m\). Then there exists \(\alpha\) in \(\mathbb{Z}_n\) and \(\beta\) in \(\mathbb{Z}_m\) such that \(H = \langle \alpha \rangle \times \langle \beta \rangle\). Taking projection maps, we can see that \(\alpha = \gcd(a, c) \operatorname{mod} n\) and \(\beta = \gcd(b, d) \operatorname{mod} m\). Thus \(H\) is an ideal if and only if

\[
\langle (a, b), (c, d) \rangle = \langle \gcd(a, c) \rangle \times \langle \gcd(b, d) \rangle.
\]

As in Theorem 4.1, the left-hand side is easily seen to be contained in the right-hand side, and we have equality if and only if both sides have the same cardinality. The cardinality of the right-hand side is \(\operatorname{ord}(\gcd(a, c)) \operatorname{ord}(\gcd(b, d))\). The cardinality of the left-hand side can be computed using Corollary 4.5: it is given by \(\operatorname{ord}(\gcd(a, c)) | \pi_2(\ker \pi_1 | H) |\). Equating these two expressions, we conclude that \(H\) is an ideal if and only if \(\operatorname{ord}(\gcd(b, d)) = | \pi_2(\ker \pi_1 | H) |\). The left-hand side of this equation is the cardinality of the set

\[
S = \{bx + dy \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}_m,
\]

and the right-hand side is the cardinality of the set

\[
T = \{bx + dy \mid x, y \in \mathbb{Z}\ \text{such that } ax + cy = 0 \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_m.
\]

\(S\) and \(T\) have the same cardinality precisely when the image of \(\phi_{b, d}: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m\) is the same as the image of \(\phi_{b, d}\) restricted to the kernel of \(\phi_{a, c}: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n\). That happens exactly when \(\ker(\phi_{a, c})\) intersects every coset in \(\mathbb{Z} \times \mathbb{Z} / \ker(\phi_{b, d})\), which is true if and only if \((\ker \phi_{a, c})(\ker \phi_{b, d}) = \mathbb{Z} \times \mathbb{Z}\). \qed
We can get a finite-type condition that is equivalent to the one in Theorem 4.6. To get this, set \( l = \text{lcm}(m, n) \). Then given elements \( \alpha \) and \( \beta \) in \( \mathbb{Z}_n \), define the linear map \( \psi_{\alpha, \beta} : \mathbb{Z}_l \times \mathbb{Z}_l \to \mathbb{Z}_n \) as \( \psi_{\alpha, \beta}(x, y) = \alpha x + \beta y \). We now have the following corollary.

**Corollary 4.7.** The subgroup of \( \mathbb{Z}_n \times \mathbb{Z}_m \) generated by \((a, b)\) and \((c, d)\) is an ideal of \( \mathbb{Z}_n \times \mathbb{Z}_m \) if and only if

\[
|\text{ker}(\psi_{a, c})(\text{ker}(\psi_{b, d})| = nm.
\]

**Proof.** This follows from the proof of the previous theorem. Note that the maps \( \phi_{a, c} \) and \( \phi_{b, d} \) factor through \( \psi_{a, c} \) and \( \psi_{b, d} \) respectively. \( \square \)

Goursat’s theorem for more than two components [Bauer et al. 2011] has a very complicated structure, and in particular, it is not helpful to solve our problem.

5. Probability that a subgroup is an ideal

As one would expect, the above results suggest that a subgroup of a ring is rarely an ideal. Now we will make this precise by computing explicitly the probability that a randomly chosen subgroup of \( \mathbb{Z}_n \times \mathbb{Z}_m \) is an ideal using the approach and results from [Petrillo 2011]. Let \( P_R \) denote the probability that a randomly chosen subgroup of a finite ring \( R \) is an ideal. This probability is given by

\[
P_R = \frac{\text{total number of ideals in } R}{\text{total number of subgroups in } (R, +)}.
\]

Our interest is in the ring \( \mathbb{Z}_n \times \mathbb{Z}_m \). If either \( n \) or \( m \) is 1, then clearly \( P_R = 1 \). So we will assume that \( n > 1 \) and \( m > 1 \). Let \( S = \{p_1, \ldots, p_k\} \) denote the set of all distinct primes which divide \( mn \). Then the prime factorizations of \( m \) and \( n \) are

\[
m = p_1^{r_1} \cdots p_k^{r_k} \quad \text{and} \quad n = p_1^{s_1} \cdots p_k^{s_k},
\]

where the exponents are nonnegative integers, and the Chinese remainder theorem gives the decomposition

\[
\mathbb{Z}_n \times \mathbb{Z}_m = (\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_1^{s_1}}) \times \cdots \times (\mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z}_{p_k^{s_k}}).
\]

**Lemma 5.1.**

\[
P_{\mathbb{Z}_n \times \mathbb{Z}_m} = \prod_{i=1}^{k} P_{\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}},
\]

**Proof.** This follows from two facts. First, note that every ideal \( I \) in \( \mathbb{Z}_n \times \mathbb{Z}_m \) is of the form \( I = \prod_{i=1}^{k} I_i \), where \( I_i \) is an ideal of the ring \( \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}} \). Next we use a theorem of Suzuki [1951] that says if \( G_1 \) and \( G_2 \) are two finite groups with relatively prime orders, then every subgroup of \( G_1 \times G_2 \) is of the form \( H_1 \times H_2 \),
where $H_i$ is a subgroup of $G_i$. In particular, every subgroup $H$ of $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$ is of the form $\prod_{i=1}^{k} H_i$, where $H_i$ is a subgroup of $\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}$. Then we have

$$P_{\mathbb{Z}_n \times \mathbb{Z}_m} = \frac{\text{total number of ideals in } \mathbb{Z}_n \times \mathbb{Z}_m}{\text{total number of subgroups in } (\mathbb{Z}_n \times \mathbb{Z}_m, +)} = \prod_{i=1}^{k} \frac{\text{total number of ideals in } \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}}{\text{total number of subgroups in } (\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}, +)} = \prod_{i=1}^{k} P_{\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}}.
$$

In view of Lemma 5.1, it is enough to compute

$$P_{\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_i^{s_i}}}.$$

We do this in the next two lemmas, beginning by computing the number of ideals.

**Lemma 5.2.** The number of ideals in $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ is equal to $(r + 1)(s + 1)$.

**Proof.** Every ideal in $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ is of the form $a\mathbb{Z}_{p^r} \times b\mathbb{Z}_{p^s}$, where $a$ is a divisor of $p^r$ and $b$ is a divisor of $p^s$. This gives $(r + 1)(s + 1)$ for the total number of ideals. \qed

Next we have to compute the number of subgroups in $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$. This number can be obtained using the above-mentioned Goursat’s theorem.

**Lemma 5.3** [Petrillo 2011]. The total number of subgroups of $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ $(r \leq s)$ is

$$p^{r+1}((s-r+1)(p-1)+2)-((s+r+3)(p-1)+2)\over (p-1)^2.$$

**Proof sketch.** Goursat’s theorem can be greatly simplified in the case under consideration. There is a unique subgroup of order $p^k$ in $\mathbb{Z}_{p^r}$ for any $0 \leq k \leq r$ and these subgroups form a linear chain. Moreover, the group of automorphisms of $\mathbb{Z}_{p^k}$ corresponds to the units in this ring, and we have $p^k - p^{k-1}$ of them. We now have to count the 5-tuples $(A_1, B_1, A_2, B_2, \phi)$ that correspond to subgroups in Goursat’s theorem. If $|A_i/B_i| = 1$, the number of subgroups is $(r + 1)(s + 1)$ because we have $r + 1$ choices for $A_1/B_1$ and $s + 1$ choices for $A_2/B_2$ (clearly $\phi$ is trivial). If $|A_i/B_i| = p^k$ for $1 \leq k \leq r$, we have $r - k + 1$ choices for $A_1/B_1$ and $s - k + 1$ choices for $A_2/B_2$, and finally $p^k - p^{k-1}$ choices for $\phi$, so in this case we have $(r - k + 1)(s - k + 1)(p^k - p^{k-1})$ subgroups. In total we have

$$(r + 1)(s + 1) + \sum_{k=1}^{r} (r - k + 1)(s - k + 1)(p^k - p^{k-1})$$

subgroups. The rest is straightforward algebra; see [Petrillo 2011]. \qed
Combining the above lemmas, we get our formulas for $P_{\mathbb{Z}_p^r \times \mathbb{Z}_p^s}$ and $P_{\mathbb{Z}_n \times \mathbb{Z}_m}$.

**Theorem 5.4.** Let $p$ be a prime and $r, s, n, m$ be positive integers, with $r \leq s$. Then

$$P_{\mathbb{Z}_p^r \times \mathbb{Z}_p^s} = \frac{(r + 1)(s + 1)(p - 1)^2}{p^{r+1}((s - r + 1)(p - 1) + 2) - ((s + r + 3)(p - 1) + 2)},$$

$$P_{\mathbb{Z}_n \times \mathbb{Z}_m} = \prod_{i=1}^{k} \frac{(r_i + 1)(s_i + 1)(p_i - 1)^2}{p_i^{r_i+1}((|s_i - r_i| + 1)(p_i - 1) + 2) - ((s_i + r_i + 3)(p_i - 1) + 2)}.$$

We now record two special cases, which can be derived from Theorem 5.4 using routine algebra.

**Corollary 5.5.** Let $p$ be a prime and let $r$ be a positive integer. Then

$$P_{\mathbb{Z}_p^r \times \mathbb{Z}_p^r} = \frac{(r + 1)^2(p - 1)^2}{p^{r+1}(p + 1) - 2r(p - 1) - 3p + 1} \quad \text{and} \quad P_{\mathbb{Z}_p \times \mathbb{Z}_p} = \frac{4}{p + 3}.$$

It is clear from the above expressions that these probabilities are small, as expected. For instance, by choosing a large prime, the value of $P_{\mathbb{Z}_p \times \mathbb{Z}_p}$ can be made arbitrarily small. Similarly for a fixed prime $p$, the numerator of $P_{\mathbb{Z}_p^r \times \mathbb{Z}_p^r}$ is a polynomial function in $r$, whereas the denominator is an exponential function in $r$. Thus $\lim_{r \to \infty} P_{\mathbb{Z}_p^r \times \mathbb{Z}_p^r} = 0$.

The main obstruction in generalizing these formulas to the rings $R = \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ is the lack of a closed formula for the number of subgroups in $(\prod_{i=1}^{k} \mathbb{Z}_p^{n_i}, +)$ when $k \geq 3$. However, when the integers $n_i$ are all square-free, one can compute $P_R$ easily. This is because Lemma 5.1 helps us to reduce the problem of computing $P_R$ to the problem of computing $P_S$, where $S = \prod_{i=1}^{r} \mathbb{Z}_p$ for some prime $p$ and positive integer $r$ ($\leq k$). The latter is a vector space over $\mathbb{F}_p$, where subgroups are same as vector subspaces. The number of subspaces in $(S, +)$ is given by the well-known formula

$$\sum_{i=1}^{r} \binom{r}{i}_p,$$

where $\binom{r}{i}_p$ is the Gaussian binomial coefficient, which counts the number of $i$-dimensional subspaces of $\mathbb{F}_p^r$. Explicitly its value is given by

$$\binom{r}{i}_p = \frac{(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})}{(p^i - 1)(p^i - p) \cdots (p^i - p^{i-1})}.$$

Since the number of ideals in $S$ is $2^r$, we get this formula:

**Proposition 5.6.**

$$P_{\mathbb{Z}_p^r} = \frac{2^r}{\sum_{i=1}^{r} \binom{r}{i}_p}.$$
Acknowledgement

We would like to thank the referee for comments and suggestions, which we used to improve the exposition of this paper.

References

[Bauer et al. 2011] K. Bauer, D. Sen, and P. Zvengrowski, “A generalized Goursat Lemma”, preprint, 2011. arXiv 1109.0024

[Dummit and Foote 2004] D. S. Dummit and R. M. Foote, Abstract algebra, 3rd ed., Wiley, Hoboken, NJ, 2004. MR 2007h:00003 Zbl 1037.00003

[Petrillo 2011] J. Petrillo, “Counting subgroups in a direct product of finite cyclic groups”, College Math. J. 42:3 (2011), 215–222. MR 2012f:20074 Zbl 1272.97033

[Suzuki 1951] M. Suzuki, “On the lattice of subgroups of finite groups”, Trans. Amer. Math. Soc. 70 (1951), 345–371. MR 12,586b Zbl 0043.02502

[Zhao 2010] W. Zhao, “Generalizations of the image conjecture and the Mathieu conjecture”, J. Pure Appl. Algebra 214:7 (2010), 1200–1216. MR 2011e:33032 Zbl 1205.33017

[Zhao 2012] W. Zhao, “Mathieu subspaces of associative algebras”, J. Algebra 350 (2012), 245–272. MR 2859886 Zbl 1255.16018

Received: 2015-05-15 Revised: 2015-06-02 Accepted: 2015-06-17

schebol@ilstu.edu Department of Mathematics, Illinois State University, Normal, IL 61790, United States

clhenry@ilstu.edu Department of Mathematics, Illinois State University, Normal, IL 61790, United States
INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, Involve provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR
Kenneth S. Berenhaut  Wake Forest University, USA

BOARD OF EDITORS

Colin Adams  Williams College, USA  Suzanne Lenhart  University of Tennessee, USA
John V. Baxley  Wake Forest University, NC, USA  Chi-Kwong Li  College of William and Mary, USA
Arthur T. Benjamin  Harvey Mudd College, USA  Robert B. Lund  Clemson University, USA
Martin Bohner  Missouri U of Science and Technology, USA  Gaven J. Martin  Massey University, New Zealand
Nigel Boston  University of Wisconsin, USA  Mary Meyer  Colorado State University, USA
Amarjit S. Budhiraja  U of North Carolina, Chapel Hill, USA  Emil Minchev  Ruse, Bulgaria
Pietro Cerone  La Trobe University, Australia  Frank Morgan  Williams College, USA
Scott Chapman  Sam Houston State University, USA  Mohammad Sal Moslehi  Ferdowsi University of Mashhad, Iran
Joshua N. Cooper  University of South Carolina, USA  Zuhair Nashed  University of Central Florida, USA
Jem N. Corcoran  University of Colorado, USA  Ken Ono  Emory University, USA
Toka Diagana  Howard University, USA  Timothy E. O’Brien  Loyola University Chicago, USA
Michael Dorff  Brigham Young University, USA  Joseph O’Rourke  Smith College, USA
Sever S. Dragomir  Victoria University, Australia  Yuval Peres  Microsoft Research, USA
Behrouz Emami Zadeh  The Petroleum Institute, UAE  Y.-F. S. Pétermann  Université de Genève, Switzerland
Joel Foisy  SUNY Potsdam, USA  Robert J. Plemmons  Wake Forest University, USA
Errin W. Fulp  Wake Forest University, USA  Carl B. Pomerance  Dartmouth College, USA
Joseph Gallian  University of Minnesota Duluth, USA  Vadim Ponomarenko  San Diego State University, USA
Stephan R. Garcia  Pomona College, USA  Bjorn Poonen  UC Berkeley, USA
Anant Godbole  East Tennessee State University, USA  James Propp  U Mass Lowell, USA
Ron Gould  Emory University, USA  Joseph H. Przytycki  George Washington University, USA
Andrew Granville  Université Montréal, Canada  Richard Rebarber  University of Nebraska, USA
Jerrold Griggs  University of South Carolina, USA  Robert W. Robinson  University of Georgia, USA
Sat Gupta  U of North Carolina, Greensboro, USA  Filip Saidak  U of North Carolina, Greensboro, USA
Jim Haglund  University of Pennsylvania, USA  James A. Sellers  Penn State University, USA
Johnny Henderson  Baylor University, USA  Andrew J. Serge  Honorary Editor
Jim Hoste  Pitzer College, USA  Ann Trenk  Wellesley College, USA
Natalia Hritonenko  Prairie View A&M University, USA  Ravi Vakil  Stanford University, USA
Glenn H. Hurlbert  Arizona State University, USA  Antonia Vecchio  Consiglio Nazionale delle Ricerche, Italy
Charles R. Johnson  College of William and Mary, USA  Ram U. Verma  University of Toledo, USA
K. B. Kulashekara  Clemson University, USA  John C. Wierman  Johns Hopkins University, USA
Gerry Ladas  University of Rhode Island, USA  Michael E. Zieve  University of Michigan, USA

PRODUCTION
Silvio Levy, Scientific Editor

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/
© 2016 Mathematical Sciences Publishers
A combinatorial proof of a decomposition property of reduced residue systems

YOTSANAN MEEMARK AND THANAKORN PRINYASART

Strong depth and quasigeodesics in finitely generated groups

BRIAN GAPINSKI, MATTHEW HORAK AND TYLER WEBER

Generalized factorization in \(\mathbb{Z}/m\mathbb{Z}\)

AUSTIN MAHLUM AND CHRISTOPHER PARK MOONEY

Cocircular relative equilibria of four vortices

JONATHAN GOMEZ, ALEXANDER GUTIERREZ, JOHN LITTLE, ROBERTO PELAYO AND JESSE ROBERT

On weak lattice point visibility

NEIL R. NICHOLSON AND REBECCA RACHAN

Connectivity of the zero-divisor graph for finite rings

REZA AKHTAR AND LUCAS LEE

Enumeration of \(m\)-endomorphisms

LOUIS RUBIN AND BRIAN RUSHTON

Quantum Schubert polynomials for the \(G_2\) flag manifold

RACHEL E. ELLIOTT, MARK E. LEWERS AND LEONARDO C. MIHALCEA

The irreducibility of polynomials related to a question of Schur

LENNY JONES AND ALICIA LAMARCHE

Oscillation of solutions to nonlinear first-order delay differential equations

JAMES P. DIX AND JULIO G. DIX

A variational approach to a generalized elastica problem

C. ALEX SAIFESTEN AND LOGAN C. TATHAM

When is a subgroup of a ring an ideal?

SUNIL K. CHEBOLU AND CHRISTINA L. HENRY

Explicit bounds for the pseudospectra of various classes of matrices and operators

FEIXUE GONG, OLIVIA MEYERSON, JEREMY MEZA, MIHAI STOICIU AND ABIGAIL WARD