A GENERALIZED GOURSAT LEMMA

KRISTINE BAUER — DEBASIS SEN — PETER ZVENGROWSKI

ABSTRACT. In this note the usual Goursat lemma, which describes subgroups of the direct product of two groups, is generalized to describing subgroups of a direct product $A_1 \times A_2 \times \cdots \times A_n$ of a finite number of groups. Other possible generalizations are discussed and applications characterizing several types of subgroups are given. Most of these applications are straightforward, while somewhat deeper applications occur in the case of profinite groups, cyclic groups, and the Sylow p-subgroups (including infinite groups that are virtual p-groups).

1. Introduction

In Sections 11–12 of the paper written in 1889 [Gou89], the famed French mathematician É d o u a r d G o u r s a t developed what is now called Goursat's lemma (also called Goursat's theorem or Goursat's other theorem), for characterizing the subgroups of the direct product $A \times B$ of two groups A, B. It seems to have been first attributed to Goursat by J. L a m b e k in [Lam58], [Lam76], who in turn attributes H. S. M. C o x e t e r for bringing this to his attention. The lemma is elementary and a fundamental question to consider, for example it appears as Exercise 5, p. 75, in L a n g's Algebra [Lan02]. It has also been the subject of recent expository articles [Pet09], [Pet11] in an undergraduate mathematics journal. It is possible that other authors discovered the lemma independently without knowing the original reference. Indeed, one such example, related to the theory of Lie groups, occurs in 1961 in the paper of A. H a t t o r i, [Hat61, Section 2.3], now translated into English [HZ09] from the original Japanese.

Other sources that mention Goursat's lemma include papers of S. D i c k s o n [Dic69] in 1969, K. R i b e t [Rib76] in 1976, the book by R. S c h m i d t [Sch94, Chapter 1.6], the paper of D. A n d e r s o n and V. C a m i l l o in 2009 [AC09],

the preprint of A. G r e i c i u s in 2009 [Gre09], the recent paper by L. T ó t h [Tóth14], and several internet sites such as [FL10], [AEM09]. Taken together, these various sources demonstrate the applicability of Goursat's lemma to diverse branches of mathematics.

There are a number of interesting possibilities for generalizing this useful lemma. The first is to subgroups of a semi-direct product, and this is studied in [Use91]. The second is to other categories besides groups. Indeed, it is proved for modules in [Lam76], and this implies that it will hold in any abelian category by applying the embedding theorems of Lubkin-Freyd-Heron-Mitchell cf. [Mac71, p. 205]. It is proved for rings in [AC09]. The most general category in which one can hope to have a Goursat lemma is an exact Mal'cev category, cf. [FL10], and for a proof of this fact cf. [CLP93, Theorem 5.7].

In this note we examine another generalization, to the direct product of a finite number of groups. While this seems at first glance to be a triviality since we can write $A \times B \times C \approx (A \times B) \times C$, unexpected complications arise as noted by C. A r r o y o et al. in [AEM09]. The complications are overcome by considering an asymmetric version of the lemma (cf. [Sch94, Section 2]) which enables us to solve the general case in Section 3. Applications within group theory are given in Section 4. These are divided into relatively easy applications followed by a more subtle application to profinite groups, then to the cyclic subgroups of a direct product $A_1 \times \cdots \times A_n$, and finally to the Sylow p-subgroups of a subgroup G of a direct product. The conditions for Sylow p-subgroups are obtained not only for finite groups but also for virtual p-groups (groups having a subgroup that is a p-group and has finite index). An Appendix gives an example that illustrates the necessity for the asymmetric version of Goursat's lemma in order to generalize it to finite direct products.

2.   Goursat's lemma, two versions

For convenience, and to establish the notation, we start by stating the usual (symmetric) version of Goursat's lemma. Let A, B be groups and $G \leq A \times B$ be a subgroup. The neutral element of each group A and B, with slight abuse of notation, will be written 'e'. Let $\pi_1 \colon A \times B \to A$, $\pi_2 \colon A \times B \to B$ be the natural projections and $\imath_1 \colon A \to A \times B$, $\imath_2 \colon B \to A \times B$ be the usual inclusions.

THEOREM 2.1 (Goursat's lemma). *There is a bijective correspondence between subgroups G of $A \times B$ and quintuples $\{\overline{G}_1, G_1, \overline{G}_2, G_2, \theta\}$, where $G_1 \trianglelefteq \overline{G}_1 \leq A$, $G_2 \trianglelefteq \overline{G}_2 \leq B$, and $\theta \colon \overline{G}_1/G_1 \xrightarrow{\approx} \overline{G}_2/G_2$ is an isomorphism.*

As mentioned above, the proof is elementary and given as an exercise in [Lan02], it can also be found in [AC09], [Hat61]. The basic idea of the proof

is as follows. Suppose that G is a subgroup of $A \times B$. Write

$$\overline{G}_1 = \pi_1(G) = \big\{ a \in A | (a, b) \in G \text{ for some } b \in B \big\},$$
$$G_1 = \imath_1^{-1}(G) = \big\{ a \in A | (a, e) \in G \big\},$$

similarly for $\overline{G}_2$ and G_2. It is easily seen that $G_1 \trianglelefteq \overline{G}_1$, $G_2 \trianglelefteq \overline{G}_2$. The isomorphism $\theta \colon \overline{G}_1/G_1 \xrightarrow{\approx} \overline{G}_2/G_2$ is given by $\theta([a]) = [b]$, where $(a, b) \in G$ and $[a] = G_1 a$, $[b] = G_2 b$ are the respective cosets of a and b in $\overline{G}_1/G_1$, $\overline{G}_2/G_2$ (again with slight abuse of notation). It is easily checked that θ is independent of the choices of a, b. Thus G determines the quintuple $Q_2'(G) = \{\overline{G}_1, G_1, \overline{G}_2, G_2, \theta\}$.

Conversely, given a quintuple $Q' = \{\overline{G}_1, G_1, \overline{G}_2, G_2, \theta\}$ where $G_1 \trianglelefteq \overline{G}_1 \leq A$, $G_2 \trianglelefteq \overline{G}_2 \leq B$ and $\theta \colon \overline{G}_1/G_1 \xrightarrow{\approx} \overline{G}_2/G_2$, let $\Gamma_2'(Q')$ be the subgroup $p^{-1}(\mathcal{G}_\theta)$, where $\mathcal{G}_\theta \leq \overline{G}_1/G_1 \times \overline{G}_2/G_2$ is the graph of θ and $p \colon \overline{G}_1 \times \overline{G}_2 \to \overline{G}_1/G_1 \times \overline{G}_2/G_2$ is the natural surjection. The functions Q_2' and Γ_2' are inverse to each other.

DEFINITION 2.2. Motivated by the correspondence between subgroups G of $A \times B$ and the quintuples Q', we say that the quintuple $Q_2'(G)$ of Theorem 2.1 is the *Goursat quintuple* for G.

We now state an equivalent asymmetric version of the lemma cf. [Sch94, Theorem 1.6.1], which is in effect a minor variation of Theorem 2.1 but has the advantage that it generalizes easily to higher direct products, as we shall see in Section 3. An example in the Appendix shows why this asymmetric version is necessary to deal with the higher direct products.

THEOREM 2.3 (Asymmetric version of Goursat's lemma). *There is a bijective correspondence between subgroups G of $A \times B$ and quadruples $\{\overline{G}_1, \overline{G}_2, G_2, \theta_1\}$, where $\overline{G}_1 \leq A$, $G_2 \trianglelefteq \overline{G}_2 \leq B$ are arbitrary subgroups of A and B, and $\theta_1 \colon \overline{G}_1 \twoheadrightarrow \overline{G}_2/G_2$ is a surjective homomorphism.*

P r o o f. The proof is similar to that of Theorem 2.1. For any subgroup G of $A \times B$ we define $Q_2(G)$ to be the quadruple

$$Q_2(G) := \{\overline{G}_1, \overline{G}_2, G_2, \theta_1\},$$

where $\overline{G}_1$, $\overline{G}_2$ and G_2 are the first, third and fourth coordinates of $Q_2'(G)$ (cf. Theorem 2.1). The surjection θ_1 is given by $\theta_1(a) = [b]$ for $a \in \overline{G}_1$ and $(a, b) \in G$ for some $b \in \overline{G}_2$ (again easily seen to be independent of the choice of b).

Conversely, for an arbitrary quadruple $Q = \{\overline{G}_1, \overline{G}_2, G_2, \theta_1\}$, with $\overline{G}_1 \leq A$, $G_2 \trianglelefteq \overline{G}_2 \leq B$, and $\theta_1 \colon \overline{G}_1 \twoheadrightarrow \overline{G}_2/G_2$ a surjective homomorphism define
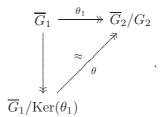
$$\Gamma_2(Q) := p^{-1}(\mathcal{G}_{\theta_1}),$$

where $\mathcal{G}_{\theta_1} \subseteq \overline{G}_1 \times \big(\overline{G}_2/G_2\big)$ is the graph of θ_1 and $p \colon \overline{G}_1 \times \overline{G}_2 \to \overline{G}_1 \times \big(\overline{G}_2/G_2\big)$ is the natural surjection. The functions Q_2 and Γ_2 are inverse to each other. $\square$

The equivalence of Theorem 2.1 and Theorem 2.3 is easily seen. It need only be pointed out that θ determines the surjection θ_1 as the composition

$$\overline{G}_1 \twoheadrightarrow \overline{G}_1/G_1 \xrightarrow[\approx]{\theta} \overline{G}_2/G_2,$$

while θ_1 determines θ via the first isomorphism theorem, specifically

$$\overline{G}_1 \xrightarrow{\theta_1} \overline{G}_2/G_2$$

$$\overline{G}_1/\mathrm{Ker}(\theta_1)$$

Finally, we have

$$\begin{aligned}
\mathrm{Ker}(\theta_1) &= \big\{a \in \overline{G}_1 | \theta_1(a) = [b], \text{with } b \in G_2\big\} \\
&= \big\{a \in \overline{G}_1 | (a,b) \in G, \ (e,b) \in G\big\} \\
&= \big\{a \in \overline{G}_1 | (a,e) \in G\big\} \\
&= G_1.
\end{aligned}$$

Remark 2.4. It is often useful to note a few additional facts, which we now list. For (a), (b) cf. [Hat61], [HZ09].

(a) $(G_1 \times G_2) \trianglelefteq G \leq \overline{G}_1 \times \overline{G}_2,$

(b) $G/(G_1 \times G_2) \approx \overline{G}_1/G_1 \approx \overline{G}_2/G_2,$

(c) From (b), using $|G_1 \times G_2| = |G_1| \cdot |G_2|$, one readily obtains that $|G| = |G_1| \cdot |\overline{G}_2| = |G_2| \cdot |\overline{G}_1|$ for the cardinality of G,

(d) One has short exact sequences of groups

$$\iota_2(G_2) = \mathrm{Ker}(\pi_1|G) \xhookrightarrow{\ \trianglelefteq\ } G \xrightarrow{\ \pi_1|G\ } \overline{G}_1 \ ,$$

$$\iota_1(G_1) = \mathrm{Ker}(\pi_2|G) \xhookrightarrow{\ \trianglelefteq\ } G \xrightarrow{\ \pi_2|G\ } \overline{G}_2 \ .$$

3. The generalized Goursat lemma

As mentioned in the Introduction, generalizing the usual Goursat lemma from $n = 2$ to $n \geq 2$ seems to create unexpected complications. However, using the asymmetric version Theorem 2.2, the generalization to finite $n \geq 2$ becomes routine. We will state the result (Theorem 3.2 below) for $n \geq 2$, after first introducing some convenient notation for any subgroup G of $A_1 \times \cdots \times A_n$.

4

DEFINITION 3.1. Let $S \subset \{1, 2, \ldots, n\} = \underline{n}$, and $j \in \underline{n} \smallsetminus S$. Then

$$G(j|S) := \big\{ x_j \in A_j | (x_1, \ldots, x_j, \ldots, x_n) \in G$$
$$\text{for some } x_i \in A_i, \ 1 \le i \le n, \ i \ne j, \ \text{with } x_i = e \text{ if } i \in S \big\}.$$

For example,

$$G(1|\emptyset) = \pi_1(G), \ G\big(1|\{2, 3, \ldots, n-1\}\big) = \big\{ x_1 \in A_1 | (x_1, e, \ldots, e) \in G \big\}.$$

These correspond to the notation used in Section 2, when $n = 2$, via $G(1|\emptyset) = \overline{G}_1$, $G(1|\{2\}) = G_1$, $G(2|\emptyset) = \overline{G}_2$, $G(2|\{1\}) = G_2$. For brevity, we extend this notation and let $\overline{G}_k := G(k|\emptyset)$ for all k. For convenience, we shall usually omit the brackets $\{\}$, e.g., $G\big(1|\{2, 3\}\big) = G(1|2, 3)$. Note that if $T \subseteq S$, then $G(j|S) \lhd G(j|T)$. As in Section 2 let $\overline{G}_i = \pi_i(G)$, where $\pi_i : A_1 \times \cdots \times A_n \twoheadrightarrow A_i$ is the standard projection onto the ith factor. Finally, it will be convenient also to use $\Pi_i : A_1 \times \cdots \times A_n \twoheadrightarrow A_1 \times \cdots \times A_i$ for the standard projection onto the first i factors, $1 \le i \le n$ (e.g., $\Pi_1 = \pi_1$ and $\Pi_n = \mathrm{id}_{A_1 \times \cdots \times A_n}$).

THEOREM 3.2 (Goursat's lemma for $n \ge 2$). *There is a bijective correspondence between the subgroups $G \le A_1 \times \cdots \times A_n$ and $(3n-2)$-tuples*

$$Q_n(G) := \big\{ \overline{G}_1, \overline{G}_2, G(2|1), \theta_1, \ldots, \overline{G}_n, G(n|1, \ldots, n-1), \theta_{n-1} \big\},$$

where $\overline{G}_i \le A_i$, $G(i|1, \ldots, i-1) \trianglelefteq \overline{G}_i$, and $\theta_i : \Lambda_i \twoheadrightarrow \overline{G}_{i+1}/G(i+1|1, \ldots, i)$ is a surjective homomorphism. Here $\Lambda_i \le A_1 \times \cdots \times A_i$ is defined recursively, $1 \le i \le n-1$, by setting $\Lambda_1 := \overline{G}_1$ and

$$\Lambda_{i+1} := \Gamma_2\big(\{\Lambda_i, \overline{G}_{i+1}, G(i+1|1, \ldots, i), \theta_i\}\big) \le (A_1 \times \cdots \times A_i) \times A_{i+1},$$

with Γ_2 as defined in Theorem 2.2.

P r o o f. Starting with G, we must construct the $(3n-2)$-tuple $Q_n(G)$, all entries of which are already defined (from G) except the θ_i. We shall show by induction, $1 \le i \le n-1$, first that $\Lambda_i = \Pi_i(G)$, and second that θ_i can then be suitably defined to successfully carry out the inductive step.

To start the induction we simply observe that by hypothesis $\Lambda_1 = \overline{G}_1$, and $\overline{G}_1 = \pi_1(G) = \Pi_1(G)$. Now suppose, as inductive hypothesis, that $\Lambda_i = \Pi_i(G)$. To define $\theta_i \colon \Lambda_i \twoheadrightarrow \overline{G}_{i+1}/G(i+1|1, \ldots, i)$, suppose $x \in \Lambda_i$. By the inductive hypothesis $x = (a_1, \ldots, a_i) \in \Pi_i(G) \le A_1 \times \cdots \times A_i$. Then $(a_1, \ldots a_i, a_{i+1}, \ldots, a_n) \in G$ for some $a_j \in A_j$, $j = i+1, \ldots, n$. We define

$$\theta_i(x) := [a_{i+1}] \in \overline{G}_{i+1}/G(i+1|1, \ldots, i).$$

To see that this definition makes sense one must check that $a_{i+1} \in \overline{G}_{i+1}$, that θ_i is surjective, and that the definition is independent of the choice of a_{i+1}.

The first two are obvious, as far as the third suppose $(a_1, \ldots, a_i, a'_i, \ldots, a'_n) \in G$. Then $\left(e, \ldots, e, a_{i+1}^{-1}a'_{i+1}, \ldots, a_n^{-1}a'_n\right) \in G$ which implies $a_{i+1}^{-1}a'_{i+1} \in G(i+1|1, \ldots \ldots, i)$ and therefore $[a_{i+1}] = [a'_{i+1}]$, i.e., θ_i is well defined. From the definitions of Λ_{i+1}, of Γ_2 (Theorem 2.2), and of θ_i, it is now obvious that $\Lambda_{i+1} = \Pi_{i+1}(G)$. This completes the inductive step.

Conversely, suppose we are given a $(3n-2)$-tuple

$$Q = \left\{\overline{G}_1, \overline{G}_2, G(2|1), \theta_1, \overline{G}_3, G(3|1,2), \theta_2, \ldots, \overline{G}_n, G(n|1,\ldots,n-1), \theta_{n-1}\right\},$$

satisfying the hypotheses of the theorem. Then simply define a subgroup $\Gamma_n(Q) \le A_1 \times \cdots \times A_n$ by $\Gamma_n(Q) := \Lambda_n$. Because Q_2 and Γ_2 are inverse to one another (cf. proof of Theorem 2.2), the iterated versions of these two operations, namely Q_n and Γ_n, are also inverse to one another. □

DEFINITION 3.3. For a subgroup $G \le A_1 \times \cdots \times A_n$, we say that the corresponding $(3n-2)$-tuple $Q_n(G)$ of Theorem 3.2 is the *Goursat decomposition* of G.

We may also refer to the Goursat quintuple of Definition 2.2 as a Goursat decomposition, even though it differs slightly from the quadruple $Q_2(G)$. In this paper the context makes clear the difference between these two possible decompositions.

Remark 3.4. As in Remark 2.3, $G \le \overline{G}_1 \times \cdots \times \overline{G}_n$. However the rest of Remark 2.3 does not directly apply here.

4. Applications

There are many potentially interesting applications of the (generalized) Goursat lemma within group theory. In this section we start with several easy applications and then explore three relatively deeper applications: profinite groups, cyclic groups and p-Sylow subgroups. For example, an immediate consequence of the lemma is that the subgroup G is a sub-direct product if and only if θ_j is the trivial homomorphism, $1 \le j \le n-1$.

PROPOSITION 4.1. *Let $\mathcal{C}$ be a class of groups closed under taking subgroups, quotient groups, and finite direct products. Let G be a subgroup of $A_1 \times \cdots \times A_n$. Then G is in the class $\mathcal{C}$ if and only if each $\overline{G}_i$ is in $\mathcal{C}$.*

P r o o f. The proposition follows from Theorem 3.2 and Remark 3.4, which taken together indicate that G is a subgroup of $\overline{G}_1 \times \cdots \times \overline{G}_n$ and furthermore each $\overline{G}_i$ is a quotient of G. □

For example, Proposition 4.1 holds for any Serre class of abelian groups and any variety of groups (in the sense of [Neu67]). In particular it holds for each of the following familiar families of groups: (a) finite groups, (b) abelian groups,

6

(c) p-groups, (d) nilpotent groups, (e) groups nilpotent of class at most m, (e) solvable groups.

To verify each of these examples, one need only verify that each class of groups satisfies the hypotheses of Proposition 4.1. This is trivial for (a), (b), (c). In (e) we find that groups which are nilpotent of class at most m are closed under subgroups and quotients as [Rot95, Theorem 5.35, 5.36]. As well, the products of groups which are nilpotent of class at most m must be nilpotent of class at most m since the commutator subgroup of the product is the product of the commutator subgroups (similarly for (d)). For (f) cf. [Rot95, Theorems 6.11, 6.12, and Corollary 6.14].

It is interesting to note that A. H a t t o r i, in [Hat61] or [HZ09], first determined the finite subgroups of the Lie group S^3 (which is isomorphic to SU(2)$\approx$ Sp(1)$\approx$ Spin(3) as a Lie group). He then applied Goursat's lemma and Proposition 4.1 to determine all finite subgroups of $S^3 \times S^3$. Using the results of Section 3 we could now, for example, find all finite subgroups of $\underbrace{S^3 \times \cdots \times S^3}_{n}$.

It is also interesting that, in fact, the papers of É. G o u r s a t [Gou89] and A. H a t t o r i [Hat61] or [HZ09] study closely related questions.

As another interesting application, which also involves some topology, we consider profinite groups. Their definition and basic properties can be found in [Ram-Val99]. Briefly, a topological group is a profinite group if it can be obtained as an inverse limit of finite groups, each having the discrete topology. Profinite groups can also be characterized as topological groups that are Hausdorff, compact, and totally disconnected. The class of profinite groups is closed with respect to taking closed subgroups, quotient groups by a closed normal subgroup, and (arbitrary) direct products. However, arbitrary subgroups of profinite groups may not be profinite, so Proposition 4.1 does not immediately apply. We shall nevertheless be able obtain a similar result by being careful about the topology.

For simplicity we start with two profinite groups A, B and a subgroup $G \leq A \times B$, where $A \times B$ has the product topology and G the subspace topology. Of course G has a Goursat decomposition $Q_2(G) = \{\overline{G}_1, \overline{G}_2, G_2, \theta_1\}$ as a group. We topologize $\overline{G}_i, i = 1, 2$, using the surjection $\pi_i : G \twoheadrightarrow \overline{G}_i$ and giving $\overline{G}_i$ the identification topology (also called the quotient topology). Then $G_1 \trianglelefteq \overline{G}_1$ is given the subspace topology. We also note that the usual projection and inclusion maps π_i, ι_i are continuous, since the product topology is being used, and that each space $\overline{G}_i, G_i$ is a subspace of either A or B, hence is Hausdorff. Note that the notation $\overline{G}_i$ is being used here as in Theorem 2.1 (definition) and subsequently, it has nothing to do with the closure operator in topology.

PROPOSITION 4.2. *Let A, B be profinite groups and $G \leq A \times B$ as above. Then G is a profinite group if an only if each of the subgroups in the Goursat decomposition for G are profinite groups and θ_1 is continuous.*

P r o o f. Suppose that G is a profinite group. Using the Hausdorff property we have $(\{e\} \times B) \bigcap G$ is a closed subgroup of G, so also profinite. But then $\pi_2 : (\{e\} \times B) \bigcap G \to G_2$ is a continuous bijection of a compact space onto a Hausdorff space, hence a homeomorphism. Since it is also a group isomorphism, G_2 is profinite, and similarly for G_1. Since $\iota_i(G_i)$ are closed normal subgroups of G, Remark 2.4 (d) and the properties of profinite groups imply that $\overline{G}_i$ are also profinite. Now consider the continuous surjective homomorphism $\mathrm{id} \times p : \overline{G}_1 \times \overline{G}_2 \twoheadrightarrow \overline{G}_1 \times (\overline{G}_2/G_2)$. Recalling that $G = (\mathrm{id} \times p)^{-1}(\mathcal{G}_{\theta_1})$, we have $\mathcal{G}_{(\theta_1)} = (\mathrm{id} \times p)(G)$. This is a continuous image of a compact space, hence compact, and hence closed since it lies in the Hausdorff space $\overline{G}_1 \times (\overline{G}_2/G_2)$. By the closed graph theorem θ_1 is continuous.

Conversely, suppose that $\overline{G}_1, \overline{G}_2, G_2$ are profinite groups, and θ_1 is continuous. Then $\overline{G}_2/G_2$ is also a profinite group. Since θ_1 is continuous, we must have (again by the closed graph theorem) that the graph $\mathcal{G}_{\theta_1} \subseteq \overline{G}_1 \times (\overline{G}_2/G_2)$ is a closed subgroup. The identification map $q : \overline{G}_1 \times \overline{G}_2 \to \overline{G}_1 \times (\overline{G}_2/G_2)$ is continuous, therefore $G = q^{-1}(\mathcal{G}_{\theta_1})$ is a closed subgroup of the profinite group $\overline{G}_1 \times \overline{G}_2$. Hence G, being a closed subgroup of a profinite group, is itself profinite. $\square$

We remark that there is a close relation between Proposition 4.2 above and [Gre09, Lemma 4.6], although neither one implies the other. It is also clear that Proposition 4.2 will generalize to subgroups of finite direct products of profinite groups with more than two factors, in the obvious way.

The next application, that of determining the cyclic subgroups of $A \times B$, will involve more substantial use of Goursat's lemma. Cyclic subgroups are not closed under products, so Proposition 4.1 does not apply. We shall henceforth use additive notation since $\overline{G}_1, G_1, \overline{G}_2, G_2$ will be abelian. One preliminary lemma will be needed.

LEMMA 4.3. *Let d divide both m and n, and let*

$$\theta : \mathbb{Z}_m/d\mathbb{Z}_m \to \mathbb{Z}_n/d\mathbb{Z}_n$$

be a given isomorphism, where both groups are, of course, isomorphic to $\mathbb{Z}_d$. Then there exist generators α, β of respectively $\mathbb{Z}_m$ and $\mathbb{Z}_n$ such that $\theta([\alpha]) = [\beta]$, where $[\alpha] = \alpha + d\mathbb{Z}_m$ and similarly $[\beta] = \beta + d\mathbb{Z}_n$.

P r o o f. We take $\alpha = 1$, and set $\theta([1]) = [\beta_0]$, so $[\beta_0]$ generates $\mathbb{Z}_n/d\mathbb{Z}_n \cong \mathbb{Z}_d$. This means that d and β_0 are coprime. In general β_0 and n need not be coprime, however $[\beta_0] = [\beta_0 + d] = [\beta_0 + 2d] = \ldots$, so it will suffice to show that $\beta_0 + kd$ is coprime to n for some k. By Dirichlet's famous theorem [Dir1837] there are infinitely many primes in the arithmetic progression $\{\beta_0 + kd\}$, so we can choose k with $p = \beta_0 + kd$ prime and also p not a divisor of n. Then p and n are coprime, and taking $\beta = p \in \mathbb{Z}_n$ fulfills the conclusion of the lemma. $\square$

Lemma 4.3 is necessary because given cyclic groups G_1 and G_2, subgroups $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$, and an isomorphism $\theta : G_1/H_1 \to G_2/H_2$, a representative $\beta \in G_2$ of $\theta([\alpha])$, α being a generator of G_1, need not generate G_2. For example, there is an isomorphism

$$\theta \colon \mathbb{Z}_{45}/9\mathbb{Z}_{45} \to \mathbb{Z}_{198}/9\mathbb{Z}_{198}$$

defined by $\theta([1]) = [2]$. But $2 \in \mathbb{Z}_{198}$ is not a generator. However, $[2] = [11] = [20] = [29]$ and although 11 and 20 are also not generators of $\mathbb{Z}_{198}$, 29 is coprime to 198 and so is a generator.

THEOREM 4.4. *Let G be a subgroup of $A \times B$ with Goursat quintuple*

$$Q'_2(G) = \{\overline{G}_1, G_1, \overline{G}_2, G_2, \theta\}.$$

(a) *The subgroup G is finite cyclic if and only if $\overline{G}_1, \overline{G}_2$ are both finite cyclic and G_1, G_2 have coprime order. Furthermore, $|G| = lcm(|\overline{G}_1|, |\overline{G}_2|)$.*

(b) *The subgroup G is infinite cyclic if and only if either $\overline{G}_1$ is infinite cyclic, $\overline{G}_2$ is finite cyclic, and $G_2 = \{0\}$, or $\overline{G}_2$ is infinite cyclic, $\overline{G}_1$ is finite cyclic, and $G_1 = \{0\}$, or both $\overline{G}_1, \overline{G}_2$ are infinite cyclic with $G_1 = G_2 = \{0\}$.*

P r o o f. In either case (*a*) or (*b*), $\overline{G}_1$ or $\overline{G}_2$ being the homomorphic image of a cyclic group, must be cyclic, hence their respective subgroups G_1, G_2 are also cyclic.

(a) Suppose G is finite cyclic, then it is generated by an element (α, β), whence $\overline{G}_1$ is cyclic and generated by α, $\overline{G}_2$ cyclic and generated by β. Let the respective orders of $\overline{G}_1, \overline{G}_2$ (i.e., of α, β) be m, n, and set $d = \gcd(m, n)$. Also write $m = m_1 d$, $n = n_1 d$. Then m_1, n_1 are coprime, and there exist $x, y \in \mathbb{Z}$ with $xm_1 + yn_1 = 1$, or equivalently $xm + yn = d$. Now $n(\alpha, \beta) = (n\alpha, 0) \in G$ implies $n\alpha \in G_1$. Also $m\alpha = 0 \in G_1$. Hence $d\alpha = (xm + yn)\alpha = x(m\alpha) + y(n\alpha) \in G_1$. It follows that $c\alpha \notin G_1$ if $0 < c < d$. For, if $c\alpha \in G_1$, then $(c\alpha, 0) \in G$. Hence $(c\alpha, 0) = z(\alpha, \beta)$ for some integer z. Therefore $z\beta = 0 = (c-z)\alpha$, whence $n|z$ and $m|(c\text{-}z)$. Since d divides m and n, we have d divides both $z, c\text{-}z$. As a result, $d|c$, which is a contradiction. Thus we conclude that G_1 is the cyclic subgroup of $\overline{G}_1$, generated by $d\alpha$ and having order $m/d = m_1$. Similarly, G_2 is generated by $d\beta$ and has order n_1, so the orders of G_1 and G_2 are coprime.

Conversely, suppose $|G_1| = m_1$ is coprime to $|G_2| = n_1$, and set $d = |\overline{G}_1|/|G_1| = |\overline{G}_2|/|G_2|$, $m = m_1 d$, $n = n_1 d$. Then $d = \gcd(m, n)$. Also $\overline{G}_1$ will be cyclic of order m, $\overline{G}_2$ cyclic of order n. Using the isomorphism $\theta \colon \overline{G}_1/G_1 \to \overline{G}_2/G_2$ and Lemma 4.3, choose generators α of $\overline{G}_1$ and β of $\overline{G}_2$ with $\theta([\alpha]) = [\beta]$. Then $[\alpha]$ and $[\beta]$ are elements of of order d, whence β has order $d|G_2| = dn_1 = n$ and generates $\overline{G}_2$. Also, by Goursat's lemma, $\gamma = (\alpha, \beta) \in G$. Finally, the order of γ is $\text{lcm}(o(\alpha), o(\beta)) = \text{lcm}(m, n) = (mn/d) = dm_1 n_1$. Further, again using Goursat's lemma, $|G| = |\mathcal{G}_\theta||G_1||G_2| = dm_1 n_1$. Thus G is cyclic of this order and generated by (α, β).

(b) Since G is infinite and $G \subseteq \overline{G}_1 \times \overline{G}_2$, at least one of $\overline{G}_1, \overline{G}_2$ must be infinite cyclic. Without loss of generality, suppose $\overline{G}_1 \approx \mathbb{Z}$. Now suppose (α, β) generates the cyclic group G, then α generates $\overline{G}_1$, and β generates $\overline{G}_2$. We claim that $G_2 = \{0\}$. For, if $y \in G_2$ then $y = r\beta$ for some integer r, whence $(0, y) = r(0, \beta) \in G$. This implies $(0, y) = k(\alpha, \beta) = (k\alpha, k\beta)$ for some integer k. Therefore $k\alpha = 0$, whence $k = 0$ and $y = k\beta = 0$. Hence $G_2 = \{0\}$. We now consider separately the cases $\overline{G}_2$ infinite and $\overline{G}_2$ finite (the case $\overline{G}_1$ finite and $\overline{G}_2 \approx \mathbb{Z}$ is symmetric to the latter, so can be omitted).

Suppose first $G \approx \mathbb{Z}$ with $\overline{G}_2 \approx \mathbb{Z}$. Then the argument in the previous paragraph now also implies $G_1 = \{0\}$. Conversely, suppose $\overline{G}_1 \approx \overline{G}_2 \approx \mathbb{Z}$ and $G_1 = G_2 = \{0\}$. Then the isomorphisms (cf. Remark 2.3)

$$G/(G_1 \times G_2) \approx \overline{G}_1/G_1 \xrightarrow{\theta} \overline{G}_2/G_2 \quad \text{reduce to} \quad G \approx \overline{G}_1 \approx \overline{G}_2 \approx \mathbb{Z}.$$

Secondly, for the remaining case, suppose $G \approx \mathbb{Z}$, $\overline{G}_1 \approx \mathbb{Z}$ as before and now $\overline{G}_2 \approx \mathbb{Z}_n$ is cyclic of order n, $n \geq 2$. Then $n(\alpha, \beta) = (n\alpha, 0)$ implies $n\alpha \in G_1$ and clearly $i\alpha \notin G_1$ if $i < n$. Thus $G_1 \approx n\mathbb{Z}$, and as before $G_2 = \{0\}$.

Conversely, suppose $\overline{G}_1 \approx \mathbb{Z}$, $G_1 \approx n\mathbb{Z}$, $\overline{G}_2 \approx \mathbb{Z}_n$ and $G_2 = \{0\}$. In this case we have the isomorphism $\theta \colon \overline{G}_1/G_1 \to \overline{G}_2/G_2 \approx \mathbb{Z}_n$. Let $\alpha \in \overline{G}_1$ with $[\alpha]$ generating $\overline{G}_1/G_1$. Then $\theta([\alpha]) = [\beta] = \beta$ generates $\overline{G}_2/G_2 = \overline{G}_2 \approx \mathbb{Z}_n$. We claim that G is generated by the single element (α, β), and thus is infinite cyclic. To see this, let $(x, y) \in G \subseteq \overline{G}_1 \times \overline{G}_2$, so $x = j\alpha, y = k\beta$ for some integers j, k. Furthermore $(x, y) \in G$ implies $\theta([x]) = [y] = y$, which gives $k\beta = y = \theta([j\alpha]) = j(\theta([\alpha])) = j\beta$. Then $j \equiv k \pmod{n}$, so $j(\alpha, \beta) = (j\alpha, j\beta) = (j\alpha, k\beta) = (x, y)$. $\qquad\square$

Theorem 4.5. *Let G be a subgroup of $A \times B \times C$ with its Goursat decomposition*

$$\{\overline{G}_1, \overline{G}_2, G(2|1), \theta_1, \overline{G}_3, G(3|1, 2), \theta_2\}.$$

(a) *The subgroup G is finite cyclic if and only if $\overline{G}_1, \overline{G}_2, \overline{G}_3$ are finite cyclic and each of the pairs of integers $(|G(1|2)|, |G(2|1)|)$, $(|G(1|3)|, |G(3|1)|)$, $(|G(2|3)|, |G(3|2)|)$ is coprime. In this case one also has*

$$|G| = lcm(|\overline{G}_1|, |\overline{G}_2|, |\overline{G}_3|).$$

(b) *The subgroup G is infinite cyclic if and only if one of the following three cases (up to obvious permutation of indices) occur:*
   (i) *$\overline{G}_1 \approx \mathbb{Z}$, $\overline{G}_2$ and $\overline{G}_3$ are finite cyclic, $G(2|1) = G(3|1) = \{0\}$, and $G(2|3), G(3|2)$ are coprime.*
   (ii) *$\overline{G}_1 \approx \overline{G}_2 \approx \mathbb{Z}$, $\overline{G}_3$ finite cyclic, and $G(2|1) = G(3|1) = G(1|2) = G(3|2) = \{0\}$.*
   (iii) *$\overline{G}_i \approx \mathbb{Z}$ for $i = 1, 2, 3$ and $G(i|j) = 0$ for $1 \leq i \neq j \leq 3$.*

P r o o f. (a) If G is finite cyclic, then so is $\overline{G}_{12} = \Pi_2(G) \subseteq A \times B$. Applying part (a) of Theorem 4.4 to $\overline{G}_{12}$ gives us $\overline{G}_1, \overline{G}_2$ finite cyclic with $|G(1|2)|$ coprime to $|G(2|1)|$. The other conditions follow by symmetry.

Conversely, suppose $\overline{G}_1, \overline{G}_2, \overline{G}_3$ are all finite cyclic with respective orders m, n, p, and that the three coprimality conditions hold. Let

$$G_{12} = \iota_{12}^{-1}(G) = \left\{ (a, b) \in \overline{G}_1 \times \overline{G}_2 | (a, b, e) \in G \right\}.$$

Applying Theorem 4.4(a) two times we obtain that $\overline{G}_{12}$ and G_{12} are both finite cyclic with respective orders $\mathrm{lcm}(m, n)$, $\mathrm{lcm}(|G(1|3)|, |G(2|3)|)$. We next apply Theorem 3.2, which tells us that G is determined by the surjection $\theta_2 \colon \overline{G}_{12} \twoheadrightarrow \overline{G}_3/G(3|1, 2)$. The third application of Theorem 4.4 (a) now tells us that G will be cyclic if $|G_{12}|$ and $|G(3|1, 2)|$ are coprime. But $|G_{12}| = \mathrm{lcm}(|G(1|3)|, |G(2|3)|)$, and $|G(3|1, 2)|$ is a divisor of $G(3|1)$ which is coprime to $|G(1|3)|$. Thus $|G(3|1, 2)|$ is coprime to $|G(1|3)|$, and similarly is coprime to $|G(2|3)|$, so also coprime to their least common multiple $|G_{12}|$.

(b) The three cases when G is infinite cyclic all follow from Theorem 4.4 (b) in obvious ways, namely in (b) (i) we use $A \times B \times C \approx A \times (B \times C)$, in (b) (ii) and (b) (iii) we use $A \times B \times C \approx (A \times B) \times C$. We omit the details. $\square$

The generalization of this theorem to $n \geq 3$ is now clear, albeit cumbersome to state since there will be many cases involved.

Determining the Sylow p-subgroups of a a group $G \leq A_1 \times \cdots \times A_n$ in terms of the Goursat decomposition of G is an application of a slightly different type. Our main result in this direction, Theorem 4.8 below, gives a very simple and natural answer to this question, and not only for finite groups but for certain classes of infinite groups. We therefore commence with a brief discussion of Sylow p-subgroups for groups that are not necessarily finite, taking p to be a fixed prime for the remainder of this section.

The Sylow p-subgroups of an arbitrary group G are easily defined as its maximal p-subgroups, which always exist by a Zorn's lemma argument. However, following [Rob82, Section 14.3], one sees that without some sort of finiteness hypothesis the familiar Sylow theorems (for a finite group) can fail badly. Indeed it is possible for two Sylow p-subgroups to even have different cardinalities, let alone be isomorphic or conjugate. One hypothesis that will insure the usual Sylow theorems hold, namely that all Sylow p-subgroups are conjugate and their number is both finite and congruent to 1 modulo p, is that there exists a Sylow p-subgroup with a finite number of conjugates. This theorem was proved in 1938 by A. P. D i e m a n, A. G. K u r o s h, A. L. U z t o v [DKU38] and in 1940 by R. B a e r [Baer40]. We shall call this finite conjugacy property "FC$_p$" and also call this theorem the "FC$_p$ theorem." We shall consider a further finiteness property, that the group is a virtual p-group, i.e., it has a p-subgroup with finite index.

It is easy to see that a virtual p-group satisfies FC_p, supposing G is a virtual p-group. Then it has a p-subgroup M of finite index, and without loss of generality (enlarging M if necessary) we may suppose M is a Sylow p-subgroup. The number of conjugates of M is given by the index $[G : N_M]$ of its normalizer N_M, and since $N_M \geq M$ this index is finite, proving the FC_p property. On the other hand, since any abelian group trivially satisfies FC_p, it is clear that FC_p does not imply that the group is a virtual p-group.

The next proposition gives us an easy way to identify a p-subgroup in a virtual p-group and along with the lemma that follows it will make the proof of the main result, Theorem 4.8 below, quite easy.
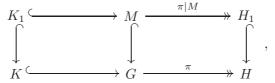
PROPOSITION 4.6. *Let G be a virtual p-group and M a p-subgroup. Then M is a Sylow p-subgroup if and only if $[G : M]$ is coprime to p.*

P r o o f. Suppose $M \leq H \leq G$, then $[G : M] = [G : H] \cdot [H : M]$. If $[G : M]$ is coprime to p, then it follows that $[H : M]$ is also coprime to p. If also H is a p-group, this can only happen if $[H : M] = 1$, whence M is a maximal p-subgroup and thus Sylow.

Conversely suppose M_1 is a Sylow p-subgroup. We have already argued above that any virtual p-group G admits a Sylow p-subgroup M having finite index. Since G also satisfies FC_p, M, M_1 are conjugate by the FC_p theorem and hence have the same index in G, so we can deal with M. Now $[G : M] = [G : N_M] \cdot [N_M : M]$, all being finite numbers. Again by the FC_p theorem, $[G : N_M] \equiv 1 \pmod{p}$, and is thus coprime to p. Since $M \trianglelefteq N_M$ and is also a Sylow p-subgroup of N_M, it is easy to see that $[N_M : M]$ is also coprime to p by considering the finite group $N_M/M := A$ which has order $[N_M : M]$, and the surjection $N_M \twoheadrightarrow A$ (the Sylow p-subgroup of A must be trivial, otherwise its inverse image would be a p-subgroup of N_M strictly larger than M). $\square$

The next lemma is a "non-commutative" version of a result that is familiar in abelian categories, where it follows at once by taking the quotient objects to form the third exact row in the diagram.

LEMMA 4.7. *Let G be any group, M any subgroup, and π a surjective homomorphism of G onto a group H. Consider the commutative diagram*

$$
\begin{array}{ccccc}
K_1 & \hookrightarrow & M & \xrightarrow{\pi|M} & H_1 \\
\downarrow & & \downarrow & & \downarrow \\
K & \hookrightarrow & G & \xrightarrow{\pi} & H
\end{array} ,
$$

where K, K_1 are the respective kernels of $\pi, \pi|M$, and H_1 is the image of $\pi|M$. Then one has the following relation of (possibly infinite) cardinal numbers: $[G : M] = [H : H_1] \cdot [K : K_1]$.

P r o o f. Since $K \trianglelefteq G$, it is standard, cf. [Rot95, Theorem 2.13], that $KM = MK = K \vee M$ is a subgroup of G. Another standard fact is that $[G : M] = [G : MK] \cdot [MK : M]$, cf. [Rob82, Section 1.3.5]. The plan of this proof is to show that $[G : MK] = [H : H_1]$ and $[MK : M] = [K : K_1]$, which will complete the proof.

For $[G : MK]$ let us first note that $MK = \pi^{-1}(H_1)$. Then $[G : MK] = [H : H_1]$ is part of [Hall59, Theorem 2.3.4].

For $[MK : M]$, let $K = \bigsqcup x_i K_1$ be a coset decomposition of K, where $x_i \in K$, $i \in \mathcal{I}$, and $x_i^{-1} x_j \in K_1$ if and only if $i = j$. By definition $|\mathcal{I}| = [K : K_1]$. Now consider $\bigcup x_i M \subseteq MK$. Now $x_i^{-1} x_j \in M$ implies $x_i^{-1} x_j \in K \cap M = K_1$, which implies $i = j$. Hence $\bigcup x_i M = \bigsqcup x_i M \subseteq MK$. Further, if $g \in MK = KM$, then $g = km = x_i k_1 m$ for some $k \in K, m \in M$, and $k = x_i k_1$ for some $i \in \mathcal{I}$ and some $k_1 \in K_1$ (given k, i and k_1 are unique). Thus $g = x_i(k_1 m) \in \bigsqcup x_i M$, showing that $MK = \bigsqcup x_i M$ from which $[MK : M] = |\mathcal{I}| = [K : K_1]$. □

COROLLARY 4.8. *Let G be a virtual p-group. Then any normal subgroup K or any quotient group H is also a virtual p-group.*

P r o o f. Given a normal subgroup K let $H = G/K$, or given a quotient group H let K equal the kernel of the projection map $G \twoheadrightarrow H$. Also, let M be a p-subgroup of G with finite index. This gives exactly the situation of Lemma 4.6, and since $[G : M]$ is finite the lemma implies that both $[K : K_1]$, $[H : H_1]$ are finite. Clearly K_1 and H_1 are p-groups since M is a p-group. Thus K and H are virtual p-groups. □

THEOREM 4.9. *Let $G \leq A \times B$ be a virtual p-group.*

  (a) *If M is a Sylow p-subgroup of G, then $\overline{M}_i$ is a Sylow p-subgroup of $\overline{G}_i$ and M_i is a Sylow p-subgroup of G_i.*

  (b) *Conversely, if $N \leq G$ has Goursat quintuple $(\overline{N}_1, N_1, \overline{N}_2, N_2, \theta_N)$ with $\overline{N}_i$ a Sylow p-subgroup of $\overline{G}_i$ and N_i a Sylow p-subgroup of G_i, then N is a Sylow p-subgroup of G.*

P r o o f. First, for both parts of the proof, notice that G being a virtual p-group implies, by Remark 2.3 (d) and Corollary 4.7, that $\overline{G}_i$ and $G_i \approx \iota_i(G_i)$, $i = 1, 2$, are also virtual p-groups.

(a) Let M be a Sylow p-subgroup of G, then $[G : M]$ is coprime to p by Proposition 4.5. Applying Lemma 4.6 to Remark 2.3 (d), with π replaced by π_1, H_1, H replaced respectively by $\overline{M}_1, \overline{G}_1$, and K_1, K replaced respectively (up to isomorphism) by M_2, G_2, we obtain $[G : M] = [\overline{G}_1 : \overline{M}_1] \cdot [G_2 : M_2]$. Hence $[\overline{G}_1 : \overline{M}_1], [G_2 : M_2]$ are also coprime to p. Since M is a p-group so are $\overline{M}_1, M_2$, and since we have already observed that $\overline{G}_1, G_2$ are virtual p groups, Proposition 4.5 implies that $\overline{M}_1, M_2$ are respectively Sylow p-subgroups of $\overline{G}_1, G_2$. The proof for $\overline{M}_2, M_1$ is similar.

(b) Conversely, given the hypotheses of (b), N must first of all be a p-group by Proposition 4.1 (c). The steps for proving (a) above can now all be reversed to show that $[G : N]$ is coprime to p, and hence by Proposition 4.5 N is a Sylow p-subgroup of G. $\qquad\square$

Using the correspondence between the symmetric and asymmetric versions of Goursat's lemma (Section 2) and Theorem 3.2, the generalization of Theorem 4.8 to subgroups of a finite direct product is clear and we simply state it here without proof.

THEOREM 4.10. *Let $G \leq A_1 \times \cdots \times A_n$ be a virtual p-group and have Goursat decomposition*

$$Q_n(G) = \left\{ \overline{G}_1, \overline{G}_2, G(2|1), \theta_1, \ldots, \overline{G}_n, G(n|1, \ldots, n-1), \theta_{n-1} \right\}$$

as in Theorem 3.2.

(a) *If M is a Sylow p-subgroup of G, then $\overline{M}_i$ is a Sylow p-subgroup of $\overline{G}_i$ and $M(i|1, \ldots i-1)$ is a Sylow p-subgroup of $G(i|1, \ldots i-1)$, $2 \leq i \leq n$.*

(b) *Conversely, if $N \leq G$ has Goursat $(2n-3)$-tuple*

$$\left\{ \overline{N}_1, \overline{N}_2, N(2|1), \varphi_1, \overline{N}_3, N(3|1, 2), \varphi_2, \ldots, \overline{N}_n, N(n|1, \ldots, n-1), \varphi_{n-1} \right\}$$

with each $\overline{N}_i$ a Sylow p-subgroup of $\overline{G}_i$ and each $N(i|1, \cdots i-1)$ a Sylow p-subgroup of $G(i|1, \ldots i-1)$, $2 \leq i \leq n$, then N is a Sylow p-subgroup of G.

We close this section with two questions.

Remark 4.11. (a) One can ask whether Theorems 4.8, 4.9 hold under the weaker hypothesis that G is an FC_p group. The answer is *no*. Let G be the infinite cyclic subgroup of $\mathbb{Z} \times \mathbb{Z}_3$ generated by $(1, 1)$, $p = 3$, and recall that any abelian group satisfies FC_p. The Sylow 3-subgroup M of G equals $\{0\}$, hence $\overline{M}_1 = \{0\}$ whereas $\overline{G}_2 = \mathbb{Z}_3$ has Sylow 3-subgroup $\mathbb{Z}_3$.

(b) In Corollary 4.7 we have seen that any normal subgroup of a virtual p-group is also a virtual p-group. Does this hold for any subgroup?
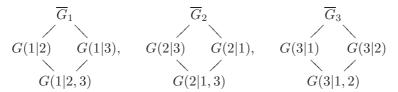
5. Appendix : An example illustrating the necessity of the asymmetric Goursat lemma

When moving from Goursat's lemma to the asymmetric version of Goursat's lemma in Section 2, we used the first isomorphism theorem to show that the required isomorphism
$$\theta \colon \overline{G}_1/G_1 \xrightarrow{\approx} \overline{G}_2/G_2$$
corresponds uniquely to the surjection
$$\theta_1 \colon \overline{G}_1 \twoheadrightarrow \overline{G}_2/G_2.$$

Now that we have derived Goursat's lemma for $n \geq 2$, it is tempting to use analogous reasoning to try to obtain a symmetric version of the lemma for $n \geq 3$. For $n = 3$, such a lemma would make use of the three lattices of subgroups, each subgroup being normal in the one above it (and using the notation of Section 3):

$$
\begin{array}{ccc}
\overline{G}_1 & \overline{G}_2 & \overline{G}_3 \\
\diagup \; \diagdown & \diagup \; \diagdown & \diagup \; \diagdown \\
G(1|2) \quad G(1|3), & G(2|3) \quad G(2|1), & G(3|1) \quad G(3|2) \\
\diagdown \; \diagup & \diagdown \; \diagup & \diagdown \; \diagup \\
G(1|2,3) & G(2|1,3) & G(3|1,2)
\end{array}
$$

together with the isomorphisms

$$
\theta : \overline{G}_1/G(1|2) \to \overline{G}_2/G(2|1),
$$
$$
\phi : \overline{G}_2/G(2|3) \to \overline{G}_3/G(3|2),
$$
$$
\psi : \overline{G}_3/G(3|1) \to \overline{G}_1/G(1|3)
$$

and also the isomorphisms

$$
\tilde{\theta} : G(1|3)/G(1|2,3) \to G(2|3)/G(2|1,3),
$$
$$
\tilde{\phi} : G(2|1)/G(2|1,3) \to G(3|1)/G(3|1,2),
$$
$$
\tilde{\psi} : G(3|2)/G(3|1,2) \to G(1|2)/G(1|2,3).
$$

The desired lemma would then state that this information uniquely determines the original subgroup G of $A \times B \times C$. In fact, this is *not* the case. Indeed, we now give an example of two subspaces of the product $A \times B \times C$ of three vector spaces, each of dimension at least 2 (say over $\mathbb{R}$ or $\mathbb{Q}$), which generate all of the same data as given above, but nevertheless, are not the same subspace, thereby showing that a symmetric version of the lemma for $n = 3$ is impossible. We remark that by applying forgetful functors this could also be considered as an example in the category of abelian groups as well as the category of groups.

Choose linearly independent vectors a_1 and a_2 in A, b_1 and b_2 in B, and c_1 and c_2 in C. Consider the 3-dimensional subspace

$$
V = \mathrm{Span}\big\{(a_1, b_1, c_1), (a_2, b_2, c_2), (a_1 + a_2, b_1 + 2b_2, c_1 + 3c_2)\big\}
$$

of $A \times B \times C$, and similarly define a second 3-dimensional subspace by

$$
V' = \mathrm{Span}\big\{(a_1, b_1, c_1 + 2c_2), (a_1, b_1 - b_2, c_1), (a_1 + 2a_2, b_1, c_1)\big\}.
$$

To compare these subspaces, we determine the twelve subspaces and nine isomorphisms presented in the subspace lattice at the beginning of this section. For example, we find that for the subspace V, an element (a, b, c) of the subspace $G(1|2) = \big\{a \in A | (a, 0, c) \in V \text{ for some } c \in C\big\}$ is determined by the

KRISTINE BAUER — DEBASIS SEN — PETER ZVENGROWSKI

existence of scalars x, y and z such that

$$a = xa_1 + ya_2 + z(a_1 + a_2)$$

and

$$0 = xb_1 + yb_2 + z(b_1 + 2b_2).$$

Since b_1 and b_2 are linearly independent, this leads us to the equations

$$x + z = 0 \quad \text{and} \quad y + 2z = 0$$

whose solutions are $x = y/2 = -z$. Thus, $a = xa_1 + ya_2 + z(a_1 + a_2) = xa_2$ and $G(1|2) = \text{Span}\{a_2\}$. In a similar fashion, we find the following subspaces of V:

$$\overline{G}_1 = \text{Span}\{a_1, a_2\}, \qquad \overline{G}_2 = \text{Span}\{b_1, b_2\}, \qquad \overline{G}_3 = \text{Span}\{c_1, c_2\},$$
$$G(1|2) = \text{Span}\{a_2\}, \qquad G(2|3) = \text{Span}\{b_2\}, \qquad G(3|1) = \text{Span}\{c_2\},$$
$$G(1|3) = \text{Span}\{a_2\}, \qquad G(2|1) = \text{Span}\{b_2\}, \qquad G(3|2) = \text{Span}\{c_2\},$$
$$G(1|2,3) = 0, \qquad G(2|1,3) = 0, \qquad G(3|1,2) = 0.$$

If we are to generalize the method of Goursat's Lemma 2.1, the isomorphism θ is determined by $\theta([a]) = [b]$ where $(a, b, c) \in V$ for some $c \in C$. Similarly, $\tilde{\theta}(a) = b$ where $(a, b, 0) \in V$ (we write $\tilde{\theta}(a)$ rather than $\tilde{\theta}([a])$ since $G(1|3)/G(1|2,3) = G(1|3)/0 = G(1|3)$, and likewise for b). The other isomorphisms ϕ, ψ, $\tilde{\phi}$ and $\tilde{\psi}$ are defined in the same manner. The fact that this produces well-defined isomorphisms is automatically determined by the definitions of the 12 subspaces in the subspace lattice. We wish to very specifically determine these isomorphisms for V, so that they can be compared to the data for V'. In this case, $\theta([a_1]) = [b_1]$ since $(a_1, b_1, c_1) \in V$ and $\theta([a_2]) = [b_2] = [0]$ since $(a_2, b_2, c_2) \in V$. The other isomorphisms are determined similarly, and we obtain:

$$\theta([a_1]) = [b_1], \qquad \phi([b_1]) = [c_1], \qquad \psi([c_1]) = [b_1],$$
$$\theta([a_2]) = [0], \qquad \phi([b_2]) = [0], \qquad \psi([c_2]) = [0],$$
$$\tilde{\theta}(a_2) = b_2/2, \qquad \tilde{\phi}(b_2) = 3c_2, \qquad \tilde{\psi}(c_2) = -a_2.$$

The determination of $\tilde{\theta}(a_2)$, for example, is given by the fact that

$$(a_2, b_2/2, 0) = \frac{1}{2}\big[(a_1, b_1, c_1) + 3(a_2, b_2, c_2) - (a_1 + a_2, b_1 + 2b_2, c_1 + 3c_2)\big]$$

is a vector in V.

We leave it as an exercise for the reader to check that all twelve subspaces and six isomorphisms corresponding to the subspace V' are exactly the same as those corresponding to V.

However, the subspaces V and V' are not the same. We offer two explanations. First, one can apply Theorem 3.2 to the subspaces V and V'. When applying this theorem, one sees from the computations above that $\overline{G}_1$, $\overline{G}_2$, $G(2|1)$, θ_1,

16

$\overline{G}_3$ and $G(3|1,2)$ are the same for each of V and V'. However, the homomorphisms $\theta_2 \colon \Gamma_2 \to \overline{G}_3/G(3|1,2)$ are not the same. The subspace Γ_2 of $A \times B$ is determined by

$$\Gamma_2 = \big\{(a,b) | (a,b,c) \in V \text{ (resp. } V') \text{ for some } c \in C \big\}$$

and the homomorphism θ_2 is defined by $\theta_2(a,b) = c$, where $(a,b,c) \in V$ (resp. V'). For V, one finds that $(a_1,b_1) \in \Gamma_2$ with $\theta_2(a_1,b_1) = c_1$ since $(a_1,b_1,c_1) \in V$. However, for V', one finds that $(a_1,b_1) \in \Gamma_2$ but $\theta_2(a_1,b_1) = c_1 + 2c_2$ since $(a_1,b_1,c_1 + 2c_2) \in V'$. Note that since $G(3|1,2) = 0$ for both V and V', there is no indeterminacy so $c_1 \neq c_1 + 2c_2$ in $\overline{G}_3$. By Theorem 3.2 we now conclude that $V \neq V'$.

A more elementary explanation is given by considering a particular case of the above example in which V and V' are both in the Grassmann manifold $G_{6,3}$ of 3-planes in $\mathbb{R}^6 = \mathbb{R}^2 \oplus \mathbb{R}^2 \oplus \mathbb{R}^2$. Let $A = B = C = \mathbb{R}^2$ and let $a_1 = b_1 = c_1 = (1,0)$ and $a_2 = b_2 = c_2 = (0,1)$. Then the subspace V is the span of

$$\big\{(1,0,1,0,1,0),(0,1,0,1,0,1),(0,1,0,2,0,3)\big\}$$

in $\mathbb{R}^6$, while V' is the span of

$$\big\{(1,0,1,0,1,2),(1,0,1,-1,1,0),(1,2,1,0,1,0)\big\}.$$

The matrix

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 & 3 \\ 1 & 0 & 1 & 0 & 1 & 2 \end{bmatrix}$$

has rank 4, showing that the vector $(1,0,1,0,1,2)$ of V' is not in V. Thus $V \neq V'$ in this case.

This demonstrates that the symmetric version of Goursat's lemma does not hold.

Remark 5.1. Upon trying to recover the symmetric version of Goursat's lemma by applying the first isomorphism theorem to Theorem 3.2, one sees almost immediately that the trouble stems from the fact that $G(1|2,3)$ is not necessarily equal to the intersection of $G(1|2)$ and $G(1|3)$, and similarly for $G(2|1,3)$ and $G(2|1,3)$. It seems very likely that a symmetric version of Goursat's lemma is available with this additional hypothesis.

REFERENCES

[AC09]   ANDERSON, D. D.—CAMILLO, V.: *Subgroups of direct products of groups, ideals and subrings of direct products of rings, and Goursat's lemma*, in: Internat. Conference on Rings and Things in honor of C. Faith and B. Osofsky (N. V. Dung et al., eds.), Zanesville, OH, USA, 2007, Contemp. Math., Vol. 480, Amer. Math. Soc., Providence, RI, 2009, pp. 1–12.

[AEM09]   ARROYO, C.—EGGLESTON, S.—MACGREGOR, B.: *Applications and generalizations of Goursat's lemma*, 2009,
            `http://www.slideshare.net/dadirac/goursats-lemma-presentation-2411944`

[Baer40]   BAER, R.: *Sylow theorems for infinite groups*, Duke J. Math. **6** (1940), 518–614.

[CLP93]   CARBONI, A.—KELLY, G. M.—PEDICCHIO, M. C.: *Some remarks on Mal'tsev and Goursat categories*, Appl. Categ. Structures **1** (1993), 385–421.

[Dic69]   DICKSON, S. E.: *On algebras of finite representation type*, Trans. Amer. Math. Soc. **135** (1969), 127–141.

[DKU38]   DIEMAN, A. P.—KUROSH, A. G.—UZKOV, A. L.: *Sylowsche Untergruppen von unendlichen Gruppen*, Mat. Sb. **3** (1938), 179–185.

[Dir1837]   DIRICHLET, P. G. L.: *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unenlich viele Primzahlen enthält*, Abhang. Ak. Wiss. Berlin **48** (1837), 45–81.

[FL10]   FARRILL, J. F.—LACK, S.: *For which categories does one have a Goursat lemma?*, 2010, `http://mathoverflow.net/questions/46700/for-which-categories-does-one-have-a-goursat-lemma`

[Gou89]   GOURSAT, É.: *Sur les substitutions orthogonales et les divisions régulières de l'espace*, Ann. Sci. École Norm. Sup. (3) **6** (1889), 9–102.

[Gre09]   GREICIUS, A.: *Elliptic curves with surjective adelic Galois representations*, arXiv:0901.2513v1, 2009.

[Hall59]   HALL, M., JR.: *The Theory of Groups.* Macmillan, New York, 1959.

[Hat61]   HATTORI, A.: *On 3-dimensional elliptic space forms*, Sūgaku **12** (1960/1961), 164–167.

[HZ09]   HATTORI, A.–MARTINS, L.–MASSAGO, S.–MIMURA, M.–ZVENGROWSKI, P.: *Three-dimensional spherical space forms*, in: Group Actions and Homogeneous Spaces (J. Korbaš et al., eds.), Proc. of the Internat. Conf., Bratislava Topology Symposium, Univ. Komenskho, Fakulta Matematiky, Fyziky a Informatiky, Bratislava, 2010, pp. 29–42.

[Lam58]   LAMBEK, J.: *Goursat's theorem and the Zassenhaus lemma*, Canad. J. Math. **10** (1958), 45–56.

[Lam76]   _____, *Lectures on Rings and Modules (2nd ed.).* Chelsea Publishing Co., New York, 1976.

[Lan02]   LANG, S.: *Algebra (3rd ed.),* in: Grad. Texts in Math., Vol. 211, Springer-Verlag, New York, 2002.

[Mac71]   MACLANE, S.: *Categories for the Working Mathematician,* in: Grad. Texts in Math., Vol. 5, Springer-Verlag, New York, 1971.

[Neu67]   NEUMANN, H.: *Varieties of Groups*, in: Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 37, Springer-Verlag, New York, 1967.

[Pet09]   PETRILLO, J.: *Goursat's other theorem*, College Math. J. **40** (2009), 119–124.

[Pet11]   _____, *Counting subgroups in a direct product of finite cyclic groups*, College Math. J. **42** (2011), 215–222.

[Ram-Val99] RAMAKRISHNAN, D.—VALENZA, R. J.: *Fourier Anaalysis on Number Fields*, in: Grad. Texts in Math., Vol. 186, Springer-Verlag, New York, 1999.

[Rib76] RIBET, K. A.: *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), 751–804.

[Rob82] ROBINSON, D.: *A Course in the Theory of Groups*, in: Grad. Texts in Math., Vol. 80, Springer-Verlag, New York, 1982.

[Rot95] ROTMAN, J.: *An Introduction to the Theory of Groups (4th ed.)*, in: Grad. Texts in Math., Vol. 148, Springer-Verlag, New York, 1995.

[Sch94] SCHMIDT, R.: *Subgroup Lattices of Groups*, in: de Gruyter Exp. Math., Vol. 14, Walter de Gruyter & Co., Berlin, 1994.

[Tóth14] TÓTH, L.: *Subgroups of finite Abelian groups having rank two via Goursat's Lemma*, Tatra Mt. Math. Publ. **59** (2014), 93–103.

[Use91] USENKO, V. M.: *Subgroups of semidirect products*, Ukrain. Mat. Zh. **43** (1991), 1048–1055.

Kristine Bauer
Peter Zvengrowski
Department of Mathematics
and Statistics
University of Calgary
Calgary, Alberta
CANADA T2N 1N4
E-mail: bauerk@ucalgary.ca
        zvengrow@ucalgary.ca

Debasis Sen
Department of Mathematics
and Statistics
Indian Institute of Technology
Kanpur
INDIA
E-mail: debasis@iitk.ac.in