PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 134, Number 10, October 2006, Pages 2795–2799
S 0002-9939(06)08396-1
Article electronically published on April 10, 2006

COUNTING ABELIAN GROUP STRUCTURES

FRANCIS CLARKE

(Communicated by Jonathan I. Hall)

Abstract. A bijective proof is given of a recurrence for the function counting the number of binary operations which endow a finite set with the structure of an abelian group. The proof depends on a lemma in "labelled homological algebra" and provides a simple route to a "curious result" of Philip Hall.

1. Introduction

The crucial element in a "curious result" due to Philip Hall [3] is a formula for the sum of the reciprocals of the orders of the automorphism groups of abelian groups whose order is a given power of a prime. This formula follows very easily from a recurrence, stated below as part (3) of Corollary 2.3, for such sums due to Henri Cohen and Hendrik Lenstra [1]. Their proof involves considering first only abelian groups with a restricted number of generators, and then letting that bound tend to infinity.

In Theorem 2.2 we restate the key recurrence which gives rise to this formula in terms of the function giving the number of binary operations on a set of cardinality n which endow the set with the structure of an abelian group. In this form we give a bijective proof for the recurrence, in which the essential ingredient is a result, Lemma 3.1, in the theory of labelled extensions.

2. AG-structures

If S is a finite set, let $\mathrm{AG}(S)$ denote the set of all binary operations $\alpha : S\times S \to S$ such that (S,α) is an abelian group. We shall refer to an element of $\mathrm{AG}(S)$ as an *AG-structure* on S. If n is a natural number, let $\mathrm{AG}(n)$ denote the cardinality of the set $\mathrm{AG}(S)$, where S is any set of cardinality n; thus $\bigl|\mathrm{AG}(S)\bigr| = \mathrm{AG}\bigl(|S|\bigr)$. We shall write $w(n) := \mathrm{AG}(n)/n!$.

If G is a given abelian group, written additively, of order n and S is a set of cardinality n, then any bijection $\phi : S \to G$ determines an element of $\mathrm{AG}(S)$ by the formula $\alpha(s,t) = \phi^{-1}\bigl(\phi(s)+\phi(t)\bigr)$. The automorphism group of G acts freely, on the left, on the set of such bijections, and it is clear that two bijections determine the same AG-structure if and only if they are in the same $\mathrm{Aut}(G)$-orbit. Thus

$$\bigl|\{\, \alpha \in \mathrm{AG}(S) : (S,\alpha) \cong G \,\}\bigr| = \frac{n!}{\bigl|\mathrm{Aut}(G)\bigr|}.$$

Received by the editors April 15, 2005.

2000 *Mathematics Subject Classification.* Primary 20K01; Secondary 20D60, 20K35, 20K40.

It follows that

$$\mathrm{AG}(n) = n! \sum_{|G|=n} \frac{1}{\bigl|\mathrm{Aut}(G)\bigr|},$$

so that

$$w(n) = \sum_{|G|=n} \frac{1}{\bigl|\mathrm{Aut}(G)\bigr|}, \tag{2.1}$$

where in these summations we take a representative from each isomorphism class of abelian groups of order n.

The main purpose of this paper is to give a bijective proof of the following result.

Theorem 2.1.

$$n\,\mathrm{AG}(n) = \sum_{d|n} \frac{n!}{d!}\,\mathrm{AG}(d).$$

Theorem 2.1 is, of course, equivalent to

Theorem 2.2 (Cohen and Lenstra [1, Theorem 3.6 (ii)])**.**

$$n\,w(n) = \sum_{d|n} w(d).$$

The following results are simple consequences of Theorem 2.2.

Corollary 2.3. (1) *The function w is multiplicative in the sense that $w(mn) = w(m)w(n)$ if m and n are coprime.*

(2)

$$w(n) = \sum_{d|n} \mu(n/d)d\,w(d),$$

where μ is the Möbius function.

(3) *If q is prime, then*

$$w(q^k) = \frac{\frac{1}{q^k}}{(1-\frac{1}{q})(1-\frac{1}{q^2})\dots(1-\frac{1}{q^k})}.$$

□

Classifying partitions according to their largest part leads directly to the following power series identity due to Euler [2, Ch. XVI]:

$$\sum_{k\geq 0} \frac{x^k}{(1-x)(1-x^2)\dots(1-x^k)} = \prod_{r\geq 1} \frac{1}{1-x^r} = \sum_{j\geq 0} p(j)x^j,$$

where p is the partition function. Since if q is prime, there are $p(k)$ isomorphism classes of abelian groups of order q^k, Philip Hall's "curious result" [3], that

$$\sum_{|G| \text{ a power of } q} \frac{1}{|G|} = \sum_{|G| \text{ a power of } q} \frac{1}{|\operatorname{Aut} G|},$$

is an immediate consequence of equation (2.1) and Corollary 2.3(3). Other proofs of Hall's result can be found in [5, 6, 7, 8].

3. A bijective proof of Theorem 2.1

Our proof depends on a result from what might be termed the theory of labelled extensions. In standard homological algebra one considers extensions up to congruence; see [4, III.1]. But here we will put no such equivalence relation on our extensions. This does, however, entail being rather more precise about what we mean by a quotient AG-structure.

Suppose then that B is a finite set and $\beta \in \mathrm{AG}(B)$. If A is a subset of B, then $\alpha \in \mathrm{AG}(A)$ is, of course, a *sub-AG-structure* of β if β restricts to α on $A \times A$.

In this situation, the standard quotient construction provides us with the following data:

(1) a partition of the set B into $|B|/|A|$ subsets, known as *cosets*, one of which is A, and each of which has cardinality $|A|$;
(2) an AG-structure on the set C of cosets, in which $A \in C$ is the zero element;
(3) a transitive action of the group (A, α) on each coset, given by $a : x \mapsto \beta(a, x)$ if $a \in A$ and $x \in X \in C$.

The following lemma answers the question of how many different elements of $\mathrm{AG}(B)$ which extend α can give rise to the same quotient structure. Its most noteworthy feature is that, unlike in classical homological algebra, the number of extensions does not depend on the group structures of the subgroup and quotient.

Lemma 3.1. *Suppose B is a finite set. Suppose the following are given:*

(1) *a partition of B into d subsets, which we will refer to as "cosets", each of which has cardinality e;*
(2) *an AG-structure on the set of cosets;*
(3) *an AG-structure on the zero coset of that structure;*
(4) *a transitive group action of the zero coset on each of the other cosets.*

Then there are e^{d-1} elements $\beta \in \mathrm{AG}(B)$ such that β restricts to the given structure on the zero coset, and provides the structure on the set of cosets and the actions of (4) *by the quotient group construction.*

Proof. Write $A \subset B$ for the zero coset, and C for the set of cosets. To simplify the notation we will write all group operations, and the action of A on each of the cosets, as addition. All zero elements will be written as 0. The context should determine which operations and which zero elements are referred to.

If we choose "coset representatives", i.e., pick a function $u : C \to B$ such that $u(X) \in X$, then, because of the action of A on each $X \in C$, an AG-structure on B with the required properties is determined once we know $u(X) + u(Y)$ for each $X, Y \in C$. Moreover, $u(X) + u(Y) \in X + Y$, so that

$$u(X) + u(Y) = u(X + Y) + f(X, Y) \tag{3.1}$$

for some $f(X, Y) \in A$.

We will only consider *normalised* coset representatives for which $u(A) = 0$, i.e., $u(0) = 0$. Then the requirements for (3.1) to define an AG-structure on B are that the function $f : C \times C \to A$ satisfies

$$f(X, 0) = 0,$$
$$f(X, Y) = f(Y, X),$$
$$f(X, Y) + f(X + Y, Z) = f(X, Y + Z) + f(Y, Z),$$

for all $X, Y, Z \in C$. Following [4, III.2 Exercise 2], let $G(C, A)$ be the set of such functions.

If another choice $v : C \to S$ of normalised coset representatives is made, then $v(X) = u(X) + h(X)$ for some function $h : C \to A$ such that $h(0) = 0$. Now if $v(X) + v(Y) = v(X + Y) + g(X, Y)$ for a function $g \in G(C, A)$, then clearly

$$g(X, Y) = f(X, Y) + h(X) + h(Y) - h(X + Y).$$

Let $R(C)$ be the set of normalised coset representatives, and let $F(C, A)$ be the set of functions $h : C \to A$ satisfying $h(0) = 0$. It is clear that $F(C, A)$ and $G(C, A)$ are abelian groups under pointwise addition in A.

The group $F(C, A)$ acts on the set $R(C) \times G(C, A)$ with $h \in F(C, A)$ sending $(u, f) \in R(C) \times G(C, A)$ to

$$\bigl(X \mapsto u(X) + h(X), (X, Y) \mapsto f(X, Y) + h(X) + h(Y) - h(X + Y)\bigr).$$

The AG-structures which we wish to count are in one-one correspondence with the orbits of this action.

Since $\bigl|F(C, A)\bigr| = \bigl|R(C)\bigr| = e^{d-1}$ and $F(C, A)$ clearly acts freely, the lemma will follow if we can show that $\bigl|G(C, A)\bigr| = e^{d-1}$. But this follows easily from elementary (classical) homological algebra. The function $\delta : F(C, A) \to G(C, A)$ given by $\delta(h) : (x, y) \mapsto h(x) + h(y) - h(x + y)$ has $\operatorname{Ker} \delta = \operatorname{Hom}(C, A)$ and $\operatorname{Coker} \delta = \operatorname{Ext}(C, A)$; see [4, III.2 Exercise 2]. From this it follows that

$$\bigl|\operatorname{Hom}(C, A)\bigr| \times \bigl|G(C, A)\bigr| = \bigl|\operatorname{Ext}(C, A)\bigr| \times \bigl|F(C, A)\bigr| = \bigl|\operatorname{Ext}(C, A)\bigr| \times e^{d-1}.$$

But it is a simple matter to check that for finite abelian groups C and A, the groups $\operatorname{Hom}(C, A)$ and $\operatorname{Ext}(C, A)$ have the same order; in fact they are (non-canonically) isomorphic. □

We may now deduce the recurrence for $\mathrm{AG}(n)$.

Proof of Theorem 2.1. Let S be a set of cardinality n. Let $(x, \alpha) \in S \times \mathrm{AG}(S)$, and suppose that x has order e in the abelian group (S, α). We can form the quotient by the subgroup $\langle x \rangle$ generated by x. Writing $n = de$, we have, in the way we have discussed, a partition of S into d cosets of cardinality e, an AG-structure on the set of cosets, a cyclic group structure on the neutral coset in which the given element x is a generator, and a transitive action of this cyclic group on each of the cosets.

There are

$$\frac{n!}{(e!)^d d!}$$

such partitions, and for each one the number of AG-structures on the set of cosets is $\mathrm{AG}(d)$. Given a partition with an AG-structure, there are $e!$ ways of choosing on the zero coset a cyclic group structure with a specified generator x, and then for each of the other cosets, there are $(e - 1)!$ ways of making this cyclic group act transitively. Having made these choices, Lemma 3.1 shows that there are e^{d-1} elements of $\mathrm{AG}(S)$ such that the quotient of (S, α) by $\langle x \rangle$ yields the chosen data. We conclude that for each divisor d of n and each $x \in S$ there are precisely $\frac{n!}{d!}\,\mathrm{AG}(d)$ elements of $\mathrm{AG}(S)$ with respect to which x has order n/d. Summing over all $x \in S$ and over all divisors of n produces the required identity. □

References

[1] Cohen, Henri and Lenstra, Hendrik W., Jr., *Heuristics on class groups of number fields*, 33–62, Number theory, Noordwijkerhout, 1983, Lecture Notes in Math. 1068, Berlin, 1984, Springer-Verlag. MR756082 (85j:11144)

[2] Euler, Leonhard, *Introductio in analysin infinitorum*, 1, Lausanne, 1748, *Opera Omnia* **8** B. G. Teubner, Geneva, 1922.

[3] Hall, Philip, *A partition formula connected with abelian groups*, Comm. Math. Helv. **11** (1938/39), 126–129.

[4] Mac Lane, Saunders, *Homology*, Grundlehren der mathematischen Wissenschaften, **114**, Springer-Verlag, Berlin, 1963. MR0156879 (28:122)

[5] Macdonald, I. G., *The algebra of partitions*, 315–333, K. W. Gruenberg, J. Roseblade, *Group theory: Essays for Philip Hall*, Academic Press, London, 1984. MR0780573 (86d:05011)

[6] Mann, Avinoam, *Philip Hall's "rather curious" formula for abelian p-groups*, Israel J. Math. **96** (1996), 445–448. MR1433700 (98a:20058)

[7] Yoshida, Tomoyuki, *P. Hall's strange formula for abelian p-groups*, Osaka J. Math. **29** (1992), 421–431. MR1181111 (93h:20057)

[8] Yoshida, Tomoyuki, *Categorical aspects of generating functions.* I. *Exponential formulas and Krull-Schmidt categories*, J. Algebra **240** (2001), 40–82. MR1830543 (2002e:18008)

Department of Mathematics, University of Wales Swansea, Swansea SA2 8PP, Wales
E-mail address: F.Clarke@Swansea.ac.uk