

3. From Theorem 3 to Theorem 1

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **49 (2003)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

3. FROM THEOREM 3 TO THEOREM 1

We first use the theorem of Eliahou and Kervaire (see Section 3 of [5]), which states that if p is an arbitrary prime, r and s two integers, then

$$(3.1) \quad \beta_p(r, s) = \mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r, s)$$

whenever $p^d \geq r, s$.

Now, from Theorem 10 of [1], it follows that μ_G coincides with $\mu_{G'}$ as soon as G and G' are two Abelian p -groups of the same order. In other words,

$$(3.2) \quad \mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r, s) = \mu_{\mathbf{Z}/p^d\mathbf{Z}}(r, s).$$

We would like to emphasize that from our method (more precisely, using simply Lemma 1) together with an inductive argument (the quotient groups of $(\mathbf{Z}/p\mathbf{Z})^d$ have the same form), we are able to derive a simple direct (that is, without using [1]) alternative proof of (3.2). Indeed, the only thing to verify is that if

$$(3.3) \quad r + s - 1 < (\lceil r/p^k \rceil + \lceil s/p^k \rceil - 1) p^k$$

for any $k \geq 1$ then we can construct sets \mathcal{A} and \mathcal{B} of respective cardinalities r and s with $|\mathcal{A} + \mathcal{B}| = r + s - 1$. This is achieved by taking for \mathcal{A} (resp. for \mathcal{B}) the r (resp. the s) smallest possible elements in the sense of the lexicographic order. Hypothesis (3.3) then ensures that, in this case, $|\mathcal{A} + \mathcal{B}| = r + s - 1$.

We are now ready to prove Theorem 1. We put for instance $d = r + s$ (but any sufficiently large d will do). Using consecutively (3.1), (3.2) and Theorem 3, we obtain

$$\begin{aligned} \beta_p(r, s) &= \mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r, s) \\ &= \mu_{\mathbf{Z}/p^d\mathbf{Z}}(r, s) \\ &= \min_{t|p^d} (\lceil r/t \rceil + \lceil s/t \rceil - 1) t \\ &= \min_{u \leq d} (\lceil r/p^u \rceil + \lceil s/p^u \rceil - 1) p^u \\ &= \min_{u \in \mathbf{N}} (\lceil r/p^u \rceil + \lceil s/p^u \rceil - 1) p^u, \end{aligned}$$

which proves Theorem 3.

ACKNOWLEDGEMENTS. I was introduced to the μ function by Shalom Eliahou during the conference “Multilinear Algebra and Matroid Theory” held in Lisboa, Portugal (March 24–26, 2002). There, he asked me for a formula for $\mu_{\mathbb{Z}/n\mathbb{Z}}$, a question which led me to Theorem 3. He then kindly indicated to me the application to the β_p functions. The author is grateful to Shalom Eliahou for his help as well as for a careful reading of preliminary versions of this paper. I would like to associate Michel Kervaire to these thanks, for the interest he took in this paper.

REFERENCES

- [1] BOLLOBAS, B. and I. LEADER. Sums in the grid. *Discrete Math.* 162 (1996), 31–48.
- [2] CAUCHY, A.L. Recherches sur les nombres. *J. École polytechnique* (1813), 99–123.
- [3] DAVENPORT, H. On the addition of residue classes. *J. London Math. Soc.* 10 (1935), 30–32.
- [4] ——— A historical note. *J. London Math. Soc.* 22 (1947), 100–101.
- [5] ELIAHOV, S. and M. KERVAIRE. Sumsets in vector spaces over finite fields. *J. Number Theory* 71 (1998), 12–39.
- [6] HOPF, H. Ein topologischer Beitrag zur reellen Algebra. *Comment. Math. Helv.* 13 (1940–41), 219–239.
- [7] HURWITZ, A. Über die Komposition der quadratischen Formen von beliebig vielen Variablen. *Nachr. Ges. Wiss. Göttingen* (1898), 309–316.
- [8] ——— Über die Komposition der quadratischen Formen. *Math. Ann.* 88 (1923), 1–25.
- [9] KNESER, M. Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z.* 58 (1953), 459–484.
- [10] PFISTER, A. Zur Darstellung von -1 als Summe von Quadraten in einem Körper. *J. London Math. Soc.* 40 (1965), 159–165.
- [11] ——— Quadratische Formen in beliebigen Körpern. *Invent. Math.* 1 (1966), 116–132.
- [12] RAJWADE, A.R. *Squares*. LMS Lecture Notes 171. Cambridge, 1993.
- [13] SHAPIRO, D. Products of sums of squares. *Exposition. Math.* 2 (1984), 235–261.
- [14] ——— *Compositions of Quadratic Forms*. Walter de Gruyter, Berlin, 2000.
- [15] STIEFEL, E. Über Richtungsfelder in den projektiven Räumen und einen Satz aus der reellen Algebra. *Comment. Math. Helv.* 13 (1940–41), 201–218.
- [16] YIU, P. On the product of two sums of 16 squares as a sum of squares of integral bilinear forms. *Quart. J. Math. Oxford Ser. (2)* 41 (1990), 463–500.