A talk given at Tongji University (Shanghai, Jan. 18, 2008)

VARIOUS EXTENSIONS OF SOME BASIC RESULTS IN COMBINATORIAL NUMBER THEORY

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Abstract. In the speaker's opinion, **a fundamental result usually has many extensions; in other words, it is the intersection of various different theorems.** In this talk we will illustrate this via some basic results and their various extensions in combinatorial number theory.

1. Three different extensions of van der Waerden's theorem

In 1927 van der Waerden established the following result conjectured by Schur, this contribution made him famous as a young mathematician.

van der Waerden Theorem. *For any positive integers k and m, if n is sufficiently large and we distribute $1,\ldots,n$ into k drawers, then some drawer contains an AP (arithmetic progression) with m terms.*

In 1933 R. Rado, one of Schur's students, proved the following theorem which includes both Schur's theorem and van der Waerden's theorem as special cases.

Theorem I.1 (Rado's Theorem). *Let $A=(a_{ij})_{1\leqslant i\leqslant m,\,1\leqslant j\leqslant n}$ be a matrix with $a_{ij}\in\mathbb{Z}$. Then the equation $A(x_1,\ldots,x_n)^T=0$ is partition regular (i.e., however we distribute all positive integers into finitely many drawers the equation always has a solution with $x_1,\ldots,x_n$ in the same drawer), if and only if we can renumber the column vectors of A so that there are integers $1\leqslant n_1<n_2<\cdots<n_l=n$ for which the sum of the first n_k $(1\leqslant k\leqslant l)$ column vectors is a rational linear combination of the first n_{k-1} column vectors, where we set $n_0=0$.*

Let S be a finite nonempty set. A *combinatorial line* in S^n has the form

$$L=\{(x_1,\ldots,x_n)\in S^n:\text{ all those }x_i\text{ with }i\in I\text{ are equal,}\\ \text{and those }x_j\text{ with }j\notin I\text{ are fixed}\},$$

where I is a nonempty subset of $[1,n]$.

In 1963 Hales and Jewett established a Ramsey-type result which stripes the van der Waerden theorem of its unessential elements and reveals the heart of Ramsey Theory.

Theorem I.2 (Hales-Jewett Theorem). *For any $m,k\in\mathbb{Z}^+$ if $n\in\mathbb{Z}^+$ is large enough then for every k-coloring of $[1,m]^n$, $[1,m]^n$ contains a monochromatic combinatorial line.*

Proof of the van der Waerden Theorem from the Hales-Jewett Theorem. Let $h=HJ(m,k)$. For $x_1,\ldots,x_h\in[1,m]$ define

$$F(x_1,\ldots,x_h)=1+\sum_{i=1}^{h-1}(x_i-1)m^i.$$

Then F is a one-to-one correspondence between $[1,m]^h$ and $[1,m^h]$. Any distribution of $1,\ldots,m^h$ into k drawers corresponds to a distribution of k-coloring of $[1,m]^h$. By the Hales-Jewett, $[1,m]^h$ contains a monochromatic combinatorial line

$$\{(x_1,\ldots,x_h)\in[1,m]^h:\ \text{those } x_i \text{ with } i\in I \text{ are equal},\ x_j=a_j \text{ for } j\notin I\},$$

where $\emptyset\ne I\subseteq[1,h]$ and $a_j\in[1,m]$ for $j\in\bar{I}=[1,h]\setminus I$. Thus, those numbers

$$1+\sum_{j\in\bar{I}}(a_j-1)m^{j-1}+\sum_{i\in I}(x-1)m^{i-1}\quad(x=1,\ldots,m)$$

lie in the same drawer. In other words, some drawer contains the arithmetic progression $a,a+d,\ldots,a+(m-1)d$, where

$$a=1+\sum_{j\in\bar{I}}(a_j-1)m^{j-1}\ \text{ and }\ d=\sum_{i\in I}m^{i-1}.$$

We are done. □

For a set $A\subseteq\mathbb{Z}^+$ we define its upper (asymptotic) density by

$$\bar{d}(A)=\limsup_{n\to\infty}\frac{|\{a\in A:\ 1\leqslant a\leqslant n\}|}{n}.$$

Note that if we distribute $1,\ldots,n$ into m drawers then some drawer contains at least δn elements where $\delta=1/m$. Thus the following deep conjecture is stronger than the van der Waerden theorem.

A Conjecture of P. Erdős and Turán (1936). *If A is a subset of $\mathbb{Z}^+$ with positive upper density, then A contains an arbitrarily long AP.*

In 1956 K. Roth proved this result for $k = 3$ by the circle method in analytic number theory. In 1969 E. Szemerédi handled the case $k = 4$ by a combinatorial method. The case of general k was settled by Szemerédi in 1975 in a paper which was regarded as "*a masterpiece of combinatorial reasoning*" by R. L. Graham. Now the conjecture is known as the famous Szemerédi theorem. Here we state another version of it.

Theorem I.3 (Szemerédi's Theorem)**.** *Let $0 < \delta \leqslant 1$ and $k \in \{3, 4, \ldots\}$. Then there is $N(k, \delta) \in \mathbb{Z}^+$ such that if $n \geqslant N(k, \delta)$ and $A \subseteq [1, n]$ with $|A| \geqslant \delta n$ then A contains an AP of length k.*

Szemerédi's theorem plays an important role in the proof of the following celebrated result.

Green-Tao Theorem. *There are arbitrarily long APs of primes.*

The Green-Tao theorem and Dirichlet's theorem (which states that if a and q are relatively prime positive integers then the arithmetic progression $a, a + q, a + 2q, \ldots$ contains infinitely many primes), are two different extensions of the infinitude of primes established by Euclid.

2. The Erdős-Heilbronn conjecture and its various extensions

Let p be a prime. Then $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a + p\mathbb{Z} : a \in \mathbb{Z}\}$ is a field with p elements. If $A = \{\bar{0}, \ldots, \overline{k-1}\}$ and $B = \{\bar{1}, \ldots, \overline{l-1}\}$ with $|A| = k \leqslant p$ and $|B| = l \leqslant p$, then

$$A + B := \{a + b : a \in A \ \& \ b \in B\} = \{\bar{0}, \ldots, \overline{k+l-2}\}$$

and hence

$$|A+B| = \min\{p,\, k+l-1\} = \min\{p,\, |A|+|B|-1\}.$$

Cauchy-Davenport Theorem. *Let p be any prime. If A and B are nonempty subsets of $\mathbb{Z}_p$, then*

$$|A+B| \geqslant \min\{p,\, |A|+|B|-1\}.$$

The Cauchy-Davenport theorem was first proved by A. Cauchy in 1813 and then rediscovered by H. Davenport [J. London Math. Soc.] in 1935. It plays a fundamental role in additive combinatorics.

The additive group $\mathbb{Z}_p$ is a cyclic group of order p. The following result extends the Cauchy-Davenport theorem to any finite group.

Theorem II.1 (G. Károlyi, 2005)**.** *Let G be any finite group written additively. Let $p(G)$ be the least order of a nonzero element of G, or $p(G) = +\infty$ if G is torsion-free. Then, for any finite nonempty subsets A and B of G, we have*

$$|A+B| \geqslant \min\{p(G), |A|+|B|-1\}.$$

Recently, Zhi-Wei Sun extended the Cauchy-Davenport theorem in another way.

Theorem II.2 (Z. W. Sun, Finite Fields Appl., in press)**.** *Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F, and let*

$$f(x_1, \ldots, x_n) = c_1 x_1^k + \cdots + c_n x_n^k + g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$$

with $k\in\mathbb{Z}^+=\{1,2,3,\ldots\}$, $c_1,\ldots,c_n\in F\setminus\{0\}$ *and* $\deg g<k$. *Then*

$$\begin{aligned}&|\{f(a_1,\ldots,a_n):\ a_1\in A_1,\ldots,a_n\in A_n\}|\\&\geqslant\min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.\end{aligned}$$

When $k=1$, $n=2$ and $F=\mathbb{Z}_p$, Theorem 2.2 yields the classical Cauchy-Davenport theorem.

In 1964 P. Erdős and H. Heilbronn [Acta Arith.] made the following challenging conjecture.

Erdős-Heilbronn Conjecture. *Let p be a prime, and let A be a subset of the field $\mathbb{Z}_p$. Then $|2^\wedge A|\geqslant\min\{p,2|A|-3\}$, where*

$$2^\wedge A=A\dot{+}A=\{a+b:\ a,b\in A,\ \text{and } a\neq b\}.$$

This conjecture is so difficult that it had been open for thirty years until it was finally confirmed by Dias da Silva and Y. Hamidoune [Bull. London. Math. Soc. 1994], with the help of the representation theory of groups.

Theorem III.1 (Dias da Silva & Hamidoune, Bull. London Math. Soc. 1994)**.** *Let F be a field and n be a positive integer. Then for any finite subset A of F we have*

$$|n^\wedge A|\geq\min\{p(F),\ n|A|-n^2+1\},$$

where $n^\wedge A$ denotes the set of all sums of n distinct elements of A.

It should be mentioned that if $A_1, \dots, A_n$ are subsets of a field F with cardinality k then

$$|A_1 \dot{+} A_2 \dot{+} \cdots \dot{+} A_n| \geqslant \min\{p(F),\ kn - n^2 + 1\},$$

but **the Dias da Silva-Hamidoune method does not work for this result**. However this follows from the following extension of the Erdős-Heilbronn conjecture obtained by the so-called Combinatorial Nullstellensatz (see, Alon [Comb. Probab. Comput. 1999]).

Theorem III.2 (Alon-Nathanson-Ruzsa, J. Number Theory, 1996)**.** *Let $A_1, \dots, A_n$ be finite nonempty subsets of a field F with $|A_1| < \cdots < |A_n|$. Then, for the restricted sumset*

$$A_1 \dot{+} \cdots \dot{+} A_n = \{a_1 + \cdots + a_n :\ a_1 \in A, \dots, a_n \in A_n,\ \text{and } a_i \neq a_j \text{ if } i \neq j\},$$

we have

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant \left\{p(F),\ \sum_{i=1}^{n}(|A_i| - i) + 1\right\}.$$

If $A_1, \dots, A_n$ are sets with cardinality $k \geqslant n$, then we can choose $A_1' \subseteq A_1, \dots, A_n' \subseteq A_n$ with cardinalities $k - n + 1, k - n + 2, \dots, k$ respectively. So Theorem III.1 follows from Theorem III.2.

Here is a further extension to polynomials of higher degrees.

Theorem III.3. *Let $A_1, \dots, A_n$ be finite nonempty subsets of F, and let*

$$f(x_1, \dots, x_n) = c_1 x_1^k + \cdots + c_n x_n^k + g(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$$

with $k \in \mathbb{Z}^+$, $c_1, \dots, c_n \in F \setminus \{0\}$ and $\deg g < k$.

(i) (Sun [Finite Fields Appl., in press]) *If $k\geqslant n$ and $|A_i|\geqslant i$ for $i=1,\ldots,n$, then*

$$|\{f(a_1,\ldots,a_n):\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i\neq a_j \text{ if } i\neq j\}|$$
$$\geqslant \min\left\{p(F),\ \sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\}.$$

(ii) (Pan & Sun, `arXiv:0801.0080`) *Assume that $c_1=\cdots=c_n=1$. Then*

$$|\{f(a_1,\ldots,a_n):\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i\neq a_j \text{ if } i\neq j\}|$$
$$\geqslant \min\{p(F),\ q_1+\cdots+q_n+1\},$$

where

$$q_i=\min_{\substack{i\leqslant j\leqslant n\\ j\equiv i\ (\mathrm{mod}\ k)}}\left\lfloor\frac{|A_j|-j}{k}\right\rfloor\quad \text{for } i=1,\ldots,n.$$

Consequently, if $|A_1|=\cdots=|A_n|=m\geqslant n$ then

$$|\{f(x_1,\ldots,x_n):\ x_1\in A_1,\ldots,x_n\in A_n, \text{and } x_i\neq x_j \text{ if } i\neq j\}|$$
$$\geqslant \min\left\{p(F),\ \frac{n(m-n)}{k}-k\left\{\frac{n}{k}\right\}\left\{\frac{m-n}{k}\right\}+r_k(m,n)+1\right\},$$

where $\{\alpha\}$ denotes the fractional part of a real number α, and

$$r_k(m,n)=\begin{cases}k\{m/k\} & \text{if } \{m/k\}<\{n/k\},\\ 0 & \text{otherwise.}\end{cases}$$

Recently P. Balister and J. P. Wheeler extended the Erdős -Heilbronn conjecture to any finite group via several ingenious steps.

Theorem III.4 (P. Balister & Wheeler, Acta Arith., to appear)**.** *Let G be any finite group written additively. Then, for any nonempty subsets A and B, we have*

$$|A \dot{+} B| \geqslant \min\{p(G),\, |A| + |B| - 3\}.$$

One of the needed lemmas is the following famous result.

Feit-Thompson Theorem (1963)**.** *Every group of odd order is solvable.*

3. The Erdős-Ginzurgh-Ziv theorem and its weighted generalizations

The following famous result was established in 1961, and it has stimulated lots of further researches on zero-sum sequences.

Erdős-Ginzburg-Ziv Theorem. *Let n be any positive integer, and let Let $c_1, \ldots, c_{2n-1} \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Then $\sum_{s\in I} c_s = 0$ for some $I \subseteq \{1, \ldots, k\}$ with $|I| = n$; in other words, the sequence $\{c_i\}_{i=1}^{2n-1}$ has a zero-sum subsequence of length n.*

The EGZ theorem can be reduced to the case where n is a prime (and hence $\mathbb{Z}_n$ is a field), and then deduced from the Cauchy-Davenport theorem or the Chevalley-Warning theorem.

The following sophisticated result is a weighted form of the EGZ theorem.

Theorem IV.1 (Conjectured by Y. Caro in 1996, and proved by D. J. Grynkiewicz [Combinatorica, 2006])**.** *Let $c_1, \ldots, c_{2n-1} \in \mathbb{Z}_n$, and let*

$w, \ldots, w_n \in \mathbb{Z}_n$ with $w_1+\cdots+w_n = 0$. Then there are distinct $j_1, \ldots, j_n \in \{1, \ldots, 2n-1\}$ such that $\sum_{i=1}^n w_i c_{j_i} = 0$.

In Grynkiewicz's proof of the weighted EGZ theorem, the following important result of Kneser plays a key role.

Kneser's Theorem (Kneser, 1953)**.** *Let G be an additive abelian group. Let A and B be finite nonempty subsets of G, and let $H = H(A+B)$ be the stabilizer $\{g \in G : g + A + B = A + B\}$. If $|A+B| \leqslant |A| + |B| - 1$, then*

$$|A+B| = |A+H| + |B+H| - |H|.$$

Now we turn to another weighted extension of the EGZ theorem involving covers of the integers by residue classes.

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ we let

$$a(n) = a + n\mathbb{Z} = \{a + nq : q \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \equiv a \pmod n\}.$$

Thus $0(1)$ coincides with $\mathbb{Z}$, and $1(2)$ is the set of odd integers.

A finite system $A = \{a_s(n_s)\}_{s=1}^k$ of residue classes is called a *cover* of $\mathbb{Z}$ or a *covering system* if $\bigcup_{s=1}^k a_s(n_s) = \mathbb{Z}$. Covers of $\mathbb{Z}$ were first introduced by P. Erdős in the early 1930s. He noted that

$$\{0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)\}$$

is a cover of $\mathbb{Z}$ with the moduli $2, 3, 4, 6, 12$ distinct.

Here is a weighted extension of the EGZ theorem involving covers of $\mathbb{Z}$.

Theorem IV.2 (Z. W. Sun, Israel J. Math., in press)**.** *Let G be an abelian group of prime power order. If $A=\{a_s(n_s)\}_{s=1}^k$ covers each integer either $2|G|-1$ times or $2|G|$ times, then for any $c_1,\ldots,c_k\in G$ there is an $I\subseteq\{1,\ldots,k\}$ such that $\sum_{s\in I}c_s=0$ and $\sum_{s\in I}1/n_s=|G|$.*

When A consists of $2|G|-1$ copies of $0(1)$, Theorem IV.2 yields the classical EGZ theorem.

4. The Mycieski conjecture and related extensions

Let H be a subgroup of a group G with $[G:H]=k<\infty$. Then we can partition G into k left cosets $g_1H,\ldots,g_kH$, and $\{g_iH\}_{i=1}^k$ forms a disjoint cover of G by left cosets. Let $\{Ha_i\}_{i=1}^k$ be a right coset decomposition of G. Then $\{a_iG_i\}_{i=1}^k$ is a disjoint cover of G where $G_i=a_i^{-1}Ha_i$. Observe that

$$\bigcap_{i=1}^k G_i=\bigcap_{i=1}^k\bigcap_{h\in H}a_i^{-1}h^{-1}Hha_i=\bigcap_{g\in G}g^{-1}Hg$$

is the normal core H_G of H in G (H_G denotes the largest normal subgroup of G contained in H).

A Basic Theorem on Covers of Groups. *Let $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ be a finite system of left cosets in a group G where $G_1,\ldots,G_k$ are subgroups of G. Suppose that $\mathcal{A}$ forms a minimal cover G (i.e. $\mathcal{A}$ covers all the elements of G but none of its proper systems does).*

(i) (B. H. Neumann, 1954) *There is a constant c_k depending only on k such that $[G:G_i]\leqslant c_k$ for all $i=1,\ldots,k$.*

(ii) (M. J. Tomkinson, 1987) We have $[G:\bigcap_{i=1}^k G_i]\leqslant k!$ where the upper bound $k!$ is best possible.

Proof (Tomkinson). We prove (ii) by induction. (Part (ii) is stronger than part (i).)

We want to show that

$$\left[\bigcap_{i\in I}G_i:\bigcap_{i=1}^k G_i\right]\leqslant (k-|I|)! \tag{$*_I$}$$

for all $I\subseteq\{1,\ldots,k\}$, where $\bigcap_{i\in\emptyset}G_i$ is regarded as G.

Clearly $(*_I)$ holds for $I=\{1,\ldots,k\}$.

Now let $I\subset\{1,\ldots,k\}$ and assume $(*_J)$ for all $J\subseteq\{1,\ldots,k\}$ with $|J|>|I|$. Since $\{a_iG_i\}_{i\in I}$ is not a cover of G, there is an $a\in G$ not covered by $\{a_iG_i\}_{i\in I}$. Clearly $a(\bigcap_{i\in I}G_i)$ is disjoint from the union $\bigcup_{i\in I}a_iG_i$ and hence contained in $\bigcup_{j\notin I}a_jG_j$. Thus

$$a\Big(\bigcap_{i\in I}G_i\Big)=\bigcup_{\substack{j\notin I\\ a_jG_j\cap a(\bigcap_{i\in I}G_i)\neq\emptyset}}\Big(a_jG_j\cap a\Big(\bigcap_{i\in I}G_i\Big)\Big)$$

and hence

$$\left[\bigcap_{i\in I}G_i:H\right]\leqslant\sum_{j\notin I}\left[G_j\cap\bigcap_{i\in I}G_i:H\right]\leqslant\sum_{j\notin I}(k-(|I|+1))!=(k-|I|)!$$

where $H=\bigcap_{i=1}^k G_i$. This concludes the induction proof. □

Two Functions. (i) The *Mycielski function* $f:\mathbb{Z}^+\to\mathbb{N}=\{0,1,2,\ldots\}$ is defined by

$$f(p_1^{a_1}\cdots p_r^{a_r})=\sum_{i=1}^r a_i(p_i-1),$$

where $a_1, \ldots, a_r \in \mathbb{N}$, and $p_1, \ldots, p_r$ are distinct primes.

(ii) Let H be a subnormal subgroup of a group G with finite index, and

$$H_0 = H \subset H_1 \subset \cdots \subset H_n = G$$

be a composition series from H to G (i.e. H_i is maximal normal in H_{i+1} for each $0 \leqslant i < n$). If the length n is zero (i.e. $H = G$), then we set $d(G, H) = 0$, otherwise we put

$$d(G, H) = \sum_{i=0}^{n-1} ([H_{i+1} : H_i] - 1).$$

(By the Jordan–Hölder theorem, $d(G, H)$ does not depend on the choice of the composition series from H to G.)

For a subnormal subgroup H of a group G with $[G : H] < \infty$, it is known that (cf. Sun [Fund. Math., 1990; European J. Combin. 2001])

$$[G : H] - 1 \geqslant d(G, H) \geqslant f([G : H]) \geqslant \log_2[G : H],$$

and $d(G, H) = f([G : H])$ if and only if G/H_G is solvable.

Mycielski's Conjecture. (J. Mycielski, 1966) *If $\{a_i G_i\}_{i=1}^k$ is a disjoint cover of an abelian group G, then $k \geqslant 1 + f([G : G_i])$ for all $i = 1, \ldots, k$.*

Here is an extension of this result.

Theorem V.1. *Let G be a group, and let $a_1 G_1, \ldots, a_k G_k$ be left cosets of subgroups $G_1, \ldots, G_k$ of G. Suppose that $\{a_i G_i\}_{i=1}^k$ covers each element of G exactly m times.*

(i) (I. Korec [Fund. Math., 1974]) *If $m=1$ and $G_1,\ldots,G_k$ are normal in G, then $k\geqslant 1+f([G:\bigcap_{i=1}^k G_i])$.*

(ii) (Z. W. Sun [European J. Combin., 2001]) *If $G_1,\ldots,G_k$ are subnormal in G, then $k\geqslant m+d(G,\bigcap_{i=1}^k G_i)$.*

Corollary (Sun [Fund. Math., 1990])**.** *Let H be a subnormal subgroup of a group G with $[G:H]<\infty$. Then*

$$[G:H]\geqslant 1+d(G,H_G)\geqslant 1+f([G:H_G])$$

and hence

$$|G/H_G|\leqslant 2^{[G:H]-1}.$$

Proof. Let $\{Ha_i\}_{i=1}^k$ be a right coset decomposition of G where $k=[G:H]$. Then $\{a_iG_i\}_{i=1}^k$ is a disjoint cover of G where all the $G_i=a_i^{-1}Ha_i$ are subnormal in G and $\bigcap_{i=1}^k G_i=H_G$. So the desired result follows. □

Theorem V.2. *Let G be a group, and let $a_1G_1,\ldots,a_kG_k$ be left cosets of subgroups $G_1,\ldots,G_k$ of G. Suppose that $\{a_iG_i\}_{i=1}^k$ covers each element of G at least m times but none of its proper systems does.*

(i) (R. J. Simpson [Acta Arith., 1985]) *If $m=1$ and $G=\mathbb{Z}$, then $k\geqslant 1+f([G:\bigcap_{i=1}^k G_i])$.*

(ii) (Z. W. Sun [Internat. J. Math., 2006]) *If G is cyclic or $G_1,\ldots,G_k$ are normal Hall subgroups of G, then $k\geqslant m+d(G,\bigcap_{i=1}^k G_i)$.*

(iii) (G. Lettl & Z. W. Sun [Acta Arith., to appear]) *If G is abelian, then we have $k\geqslant m+f([G:G_i])$ for all $i=1,\ldots,k$.*

Note that the Lettl-Sun result in the case $m = 1$ extends the Mycielski conjecture in a new way. The "*disjoint cover*" condition is weaken while the result keeps unchanged.

Corollary (Gao-Geroldinger conjecture)**.** *Let G be a finite abelian group. If $G \setminus \{e\}$ can be written as a union of k cosets of subgroups of G, then $k \geqslant f(|G|)$.*

Proof. Let $a_1G_1, \ldots, a_kG_k$ be left cosets in G. Suppose that $\bigcup_{i=1}^{k} a_iG_i = G \setminus \{e\}$. Then $\{a_iG_i\}_{i=0}^{k}$ forms a cover of G with a_0G_0 irredundant, where $a_0 = e$ and $G_0 = \{e\}$. Applying the Lettl-Sun result we get that $k + 1 \geqslant 1 + f([G : G_0])$, i.e., $k \geqslant f(|G|)$. $\square$

We mention that the proof of the Lettl-Sun result was obtained via characters of abelian groups and algebraic number theory; below is a key lemma used for the proof.

A Lemma of Lettl and Sun ([Acta Arith., to appear])**.** *Let $n > 1$ be an integer. Then $f(n)$ is the smallest positive integer k such that there are roots of unity $\zeta_1, \ldots, \zeta_k$ different from 1 for which $\prod_{s=1}^{k}(1 - \zeta_s) \equiv 0 \pmod{n}$ in the ring of algebraic integers.*