TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 229, 1977

FIELDS GENERATED BY LINEAR COMBINATIONS OF ROOTS OF UNITY

BY

R. J. EVANS AND I. M. ISAACS([1])

ABSTRACT. It is shown that a linear combination of roots of unity with rational coefficients generates a large subfield of the field generated by the set of roots of unity involved, except when certain partial sums vanish. Some related results about polygons with all sides and angles rational are also proved.

1. **Introduction.** Let U denote the group of roots of unity in the complex numbers and let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s \in U$ be distinct. Suppose $a_1, a_2, \ldots, a_s \in \mathbf{Q}$ and assume that $\sum_{i \in T} a_i \varepsilon_i \neq 0$ for every nonempty subset $T \subseteq \{1, 2, \ldots, s\}$. Let $\alpha = \sum_{i=1}^{s} a_i \alpha_i$ and define the field $E = \mathbf{Q}(\varepsilon_1, \ldots, \varepsilon_s)$. Our main result is that the degree $d = |E : \mathbf{Q}(\alpha)|$ is bounded by some function of s, independently of the choice of the ε_i. In fact we show that $d \leq 2^{s-1}$. For $s \leq 4$ this is best possible and for arbitrary s we produce examples with $d \geq (3^{1/3})^{s-1}$. (See §4.)

We also consider convex polygons with all sides and angles rational (angles measured in degrees). Such an n-gon corresponds to an equality $\sum_{i=1}^{n} a_i \varepsilon_i = 0$ with $\varepsilon_i \in U$ and $a_i \in \mathbf{Q}$. We prove for $n \leq 5$ that either two sides of the polygon are parallel or else the figure is an equilateral triangle or a regular pentagon.

2. **The main theorem.** We introduce some notation which enables us to distinguish between formal linear combinations of roots of unity and the values of such combinations. We consider functions $f\colon U \to \mathbf{Q}$ where U is the group of roots of unity. Write $S(f) = \{u \in U \mid f(u) \neq 0\}$, the *support* of f, and define

$$\mathcal{F} = \{f\colon U \to \mathbf{Q} \mid |S(f)| < \infty\}.$$

For $f \in \mathcal{F}$, write $\Sigma(f) = \sum_{u \in S(f)} f(u)u$. Also, write $\mathbf{Q}(f) = \mathbf{Q}(S(f))$, the field generated over $\mathbf{Q}$ by the support of f. (Note that $\mathbf{Q}(f)$ is Galois over $\mathbf{Q}$ and that $\mathrm{Gal}(\mathbf{Q}(f)/\mathbf{Q})$ is abelian.) Finally, write $G(f) = \mathrm{Gal}(\mathbf{Q}(f)/\mathbf{Q}(\Sigma(f)))$.

Received by the editors November 3, 1975.
AMS (MOS) subject classifications (1970). Primary 12A35, 12F10; Secondary 50B99.
Key words and phrases. Roots of unity, rational polygon.
([1])Research partially supported by a grant from the National Science Foundation.

Thus $|G(f)| = |\mathbf{Q}(f) : \mathbf{Q}(\Sigma(f))|$ and our object is to bound $|G(f)|$ in terms of $|S(f)|$.

If $f, g \in \mathcal{F}$ and $S(f) \cap S(g) = \emptyset$, we define $f \dot{+} g \in \mathcal{F}$ by $(f \dot{+} g)(u) = f(u) + g(u)$. The following definition is the key to the proof of Theorem 2.2 (b) which is our main result.

DEFINITION 2.1. Suppose $f \in \mathcal{F}$ can be written in the form $f = g_1 \dot{+} \cdots \dot{+} g_r$ with $r > 1$ and $S(g_i) \neq \emptyset$ for $1 \leqslant i \leqslant r$ and such that $G(f)$ permutes the numbers $\Sigma(g_i)$, preserving multiplicities. In this case we say that f is *imprimitive*. If no such decomposition of f exists, then f is *primitive*.

For example, if $G(f) = 1$ and $|S(f)| > 1$, then f is imprimitive. If $S(f) = \{i, i\omega\}$ where $\omega = e^{2\pi i/3}$ and $f(i) = 1$ and $f(i\omega) = 2$, then f is primitive since $\Sigma(f) = -\sqrt{3}$ and complex conjugation does not permute i and $2i\omega$.

We need some further notation. For natural numbers n, write $U_n = \{u \in U | u^n = 1\}$ and $\mathbf{Q}_n = \mathbf{Q}(e^{2\pi i/n})$. For $f \in \mathcal{F}$, put $k(f) = \min\{k | S(f) \subseteq \mathbf{Q}_k\}$. Thus $\mathbf{Q}(f) = \mathbf{Q}_{k(f)}$ and $|\mathbf{Q}(f) : \mathbf{Q}| = \varphi(k(f))$. Also, if $u \in U$ and $f \in \mathcal{F}$, define $uf \in \mathcal{F}$ by setting $uf(ux) = f(x)$. (Thus $S(uf) = uS(f)$ and $\Sigma(uf) = u\Sigma(f)$.) Finally, if $f = g \dot{+} h$ with $S(g) \neq \emptyset$, we say that $\Sigma(g)$ is a *subsum* of f. Note that if f is primitive and $\Sigma(f) \neq 0$, then f has no zero subsum.

THEOREM 2.2. *Let $f \in \mathcal{F}$ with $\Sigma(f) \neq 0$. Put $s = |S(f)|$ and $k = k(f)$. We have*:

(a) *If f is primitive, then $\mathbf{Q}_{k/k_0} \subseteq \mathbf{Q}(\Sigma(f))$ where k_0 is the product of those prime divisors of k which are less than $2s$.*

(b) *If f has no zero subsum, then $|G(f)| \leqslant 2^{s-1}$.*

Note that when f is primitive, part (a) of the theorem yields

$$|G(f)| \leqslant \varphi(k)/\varphi(k/k_0) \leqslant k_0.$$

This bound, however, is not as good as that given in part (b). Statement (a) is included because it gives a specific large subfield of $\mathbf{Q}(\Sigma(f))$.

We will use the fact that $\prod_{p<x} p \leqslant 4^{x-1}$ for all $x \geqslant 1$, where p runs over primes. This is a slight strengthening of Theorem 415 [2]. The easy proof given there can be made to yield the desired inequality. Although stronger estimates on $\prod_{p<x} p$ are available, they do not seem to be useful for strengthening Theorem 2.2(b) because of the inductive nature of the proof.

PROOF OF THEOREM 2.2. We use induction on s. Since both (a) and (b) are trivial when $s = 1$, we assume $s > 1$. First suppose that f is primitive. Write $G = G(f)$ and $k = p^a m$ where p is a prime, $a \geqslant 1$ and $p \nmid m$.

Assume that $a > 1$ and let δ be a primitive p^ath root of unity. Write $q = p^{a-1}$. Then $1, \delta, \delta^2, \ldots, \delta^{q-1}$ are coset representatives for U_{mp} in U_k and we can write

$$f = g_0 \dot{+} \delta g_1 \dot{+} \cdots \dot{+} \delta^{q-1} g_{q-1} \tag{1}$$

where $S(g_i) \subseteq U_{mp}$. For $\sigma \in G$, we have $\sigma(\delta^i) = \mu\delta^j$ for some $\mu \in U_{mp}$ and $0 \leqslant j < q$. Write $\mu = \mu(i, \sigma)$ and $j = i \cdot \sigma$. Note that $i \mapsto i \cdot \sigma$ defines a permutation of $\{0, 1, \ldots, q-1\}$ and that $\mu(i, \sigma) \in U_{p^a} \cap U_{mp} = U_p$. We have

$$\sigma(\delta^i) = \mu(i, \sigma)\delta^{i\cdot\sigma}. \tag{2}$$

Now write $\alpha = \Sigma(f)$ and $\beta_i = \Sigma(g_i)$ so that (1) yields

$$\alpha = \sum_{i=0}^{q-1} \delta^i\beta_i \tag{3}$$

and

$$\alpha = \sigma(\alpha) = \sum_{i=0}^{q-1} \mu(i, \sigma)\delta^{i\cdot\sigma}\sigma(\beta_i) \tag{4}$$

for $\sigma \in G$.

However, $\mathbf{Q}_k = \mathbf{Q}_{mp}(\delta)$ and since $|\mathbf{Q}_k : \mathbf{Q}_{mp}| = \varphi(k)/\varphi(mp) = q$, it follows that $1, \delta, \ldots, \delta^{q-1}$ are linearly independent over $\mathbf{Q}_{mp}$. Since β_i and $\mu(i, \sigma)$ lie in $\mathbf{Q}_{mp}$, equations (3) and (4) yield

$$\beta_{i\cdot\sigma} = \mu(i, \sigma)\sigma(\beta_i). \tag{5}$$

Using (2), we obtain

$$\sigma(\delta^i\beta_i) = \mu(i, \sigma)\delta^{i\cdot\sigma}\sigma(\beta_i) = \delta^{i\cdot\sigma}\beta_{i\cdot\sigma}$$

and therefore each $\sigma \in G$ permutes the $\delta^i\beta_i = \Sigma(\delta^i g_i)$. Now equation (1) and the primitivity of f yield some i such that $S(g_j) = \varnothing$ for all $j \neq i$ and thus $f = \delta^i g_i$. Since $S(f) \not\subseteq U_{k/p}$, we see that δ^i is a primitive p^ath root of unity, and so by a change of notation, we may assume that $i = 1$.

Now $\beta_j = 0$ for $j \neq 1$ and $\beta_1 \neq 0$ since $\Sigma(f) \neq 0$. Thus (5) yields $1 \cdot \sigma = 1$ and thus $\sigma(\delta) = \mu(1, \sigma)\delta$. Since $\mu(1, \sigma)^p = 1$, we conclude that G fixes δ^p and, hence,

$$U_{p^{a-1}} \subseteq \mathbf{Q}(\Sigma(f)). \tag{6}$$

To summarize, there exist $v \in U_{p^a}$, $g \in \mathfrak{F}$ and a function $\mu: G \to U_p$ such that

$$f = vg \quad \text{and} \quad S(g) \subseteq U_{mp}, \tag{7}$$

$$\sigma(v) = v\mu(\sigma) \quad \text{for } \sigma \in G. \tag{8}$$

In the case that $a = 1$, we take $v = 1$, $g = f$ and $\mu(\sigma) = 1$ for all σ. Thus (7) and (8) remain valid.

Now in the general situation, $a \geqslant 1$, let ε be a primitive pth root of unity and write

$$g = h_0 + \varepsilon h_1 + \cdots + \varepsilon^{p-1}h_{p-1} \tag{9}$$

with $S(h_i) \subseteq U_m$. Let $\beta = \Sigma(g)$ and $\gamma_i = \Sigma(h_i)$. For $\sigma \in G$, write $\sigma(\varepsilon) = \varepsilon^{r(\sigma)}$ with $1 \leqslant r(\sigma) < p$ and $\mu(\sigma) = \varepsilon^{t(\sigma)}$ with $0 \leqslant t(\sigma) < p$ where $\mu(\sigma)$ is as in (8).

If $a = 1$, we have $\mu(\sigma) = 1$ and $t(\sigma) = 0$. If $a > 1$, we have $\varepsilon \in U_{p^{a-1}}$ and hence $r(\sigma) = 1$ by (6). Thus we have

(10) Either $r(\sigma) = 1$ for all $\sigma \in G$ or $t(\sigma) = 0$ for all $\sigma \in G$.

Also, observe that r defines a homomorphism from G into the multiplicative group of integers mod p.

For $\sigma \in G$ write $i * \sigma = j$ if $ir(\sigma) + t(\sigma) \equiv j \bmod p$ and $0 \leqslant j < p$. Thus the map $i \mapsto i * \sigma$ is a permutation of $\{0, 1, \ldots, p-1\}$. Now (7) and (9) yield

$$\alpha = v\beta = \sum_{i=0}^{p-1} v\varepsilon^i \gamma_i,$$

and using (8) we obtain

$$\alpha = \sigma(\alpha) = \sum_{i=0}^{p-1} v\varepsilon^{i * \sigma} \sigma(\gamma_i).$$

Therefore

$$0 = \sum_{i=0}^{p-1} \left(\sigma(\gamma_i) - \gamma_{i * \sigma}\right)\varepsilon^{i * \sigma} \tag{11}$$

for all $\sigma \in G$.

Now, $1, \varepsilon, \ldots, \varepsilon^{p-2}$ are linearly independent over $\mathbf{Q}_m$. Since $\sum_{i=0}^{p-1} \varepsilon^i = 0$ and all $\gamma_i \in \mathbf{Q}_m$, it follows that all of the coefficients in (11) are equal and thus

$$\sigma(\gamma_i) = \gamma_{i * \sigma} + x(\sigma) \tag{12}$$

where $x(\sigma) \in \mathbf{Q}_m$ is independent of i.

Suppose $x(\sigma) = 0$ for some $\sigma \in G$. Then

$$\sigma\left(v\varepsilon^i \gamma_i\right) = v\varepsilon^{i * \sigma} \sigma(\gamma_i) = v\varepsilon^{i * \sigma} \gamma_{i * \sigma} \tag{13}$$

and thus σ permutes the numbers $v\varepsilon^i \gamma_i = \Sigma(v\varepsilon^i h_i)$.

Assume now, that $x(\sigma) = 0$ for all $\sigma \in G$. Then equations (7) and (9) and the primitivity of f yield that $f = v\varepsilon^i h_i$ for some i and $\gamma_j = 0$ for $j \neq i$. Since $\gamma_i \neq 0$, we conclude from (13) that $i * \sigma = i$ and thus $ir(\sigma) + t(\sigma) \equiv i \bmod p$. If $r(\sigma) = 1$, this forces $t(\sigma) = 0$ and if $r(\sigma) \neq 1$, (10) yields $t(\sigma) = 0$. Hence G fixes v by (8). Also, $ir(\sigma) \equiv i \bmod p$ and thus G fixes ε^i. Therefore, $v\varepsilon^i \in \mathbf{Q}(\Sigma(f))$. Since $f = v\varepsilon^i h_i$, $S(h_i) \subseteq U_m$ and $v\varepsilon^i \in U_{p^a}$, it follows that $v\varepsilon^i$ is a primitive p^ath root of unity and thus

$$U_{p^a} \subseteq \mathbf{Q}(\Sigma(f)) \quad \text{provided all } x(\sigma) = 0. \tag{14}$$

Suppose now that $x(\sigma) \neq 0$ for some $\sigma \in G$. It follows from (12) that if $\gamma_i = 0$, then $\gamma_{i*\sigma} \neq 0$ and thus at least half of the γ_i are nonzero. Since there are at most s nonzero γ_i's, it follows that $p \leqslant 2s$.

Now (6) and (14) yield that $U_{p^{e-1}} \subseteq \mathbf{Q}(\Sigma(f))$ for all p and $U_{p^e} \subseteq \mathbf{Q}(\Sigma(f))$ for $p > 2s$. This yields part (a) of the theorem since $2s$ is not prime.

We continue with the assumption that f is primitive and proceed to prove (b) in this case. Let $\mathcal{P}$ be the set of primes p dividing k such that $U_{p^e} \not\subseteq \mathbf{Q}(\Sigma(f))$, in the notation of the first part of the proof. By (6) we have

$$|G| \leqslant \prod_{p \in \mathcal{P}} p. \tag{15}$$

If every $p \in \mathcal{P}$ satisfies $p \leqslant s/2$, then by the remark preceding the proof we have

$$|G| \leqslant 4^{(s/2)-1} \leqslant 2^{s-1}$$

as required.

Let p be maximal in $\mathcal{P}$. We may thus assume that $p > s/2$ and also by (15) that $p > 2$. We use all of the previous notation with respect to the fixed prime p.

We claim that $t(\sigma) = 0$ for all $\sigma \in G$. By (7) and (8), we have $v\beta = \alpha = \sigma(\alpha) = v\mu(\sigma)\sigma(\beta)$ and thus $\sigma(\beta) = \beta\mu(\sigma)^{-1}$. If $t(\sigma) \neq 0$, then $a > 1$ and by (6), σ fixes $\mu(\sigma) \neq 1$. It follows that β has exactly p conjugates under the action of $\langle\sigma\rangle$ and since $\beta \in \mathbf{Q}_{mp}$, we conclude that the image of the restriction map $G \to \mathrm{Gal}(\mathbf{Q}_{mp}/\mathbf{Q})$ has order divisible by p. Therefore, there exists a prime $q|m$ with $p|(q-1)$ and such that G does not fix all q-power roots of unity in $\mathbf{Q}_{mp}$. Thus $q \in \mathcal{P}$, contradicting the maximality of p. Therefore $t(\sigma) = 0$ for all $\sigma \in G$, as claimed.

Now let $H = \{\sigma \in G | r(\sigma) = 1\}$. Since r defines a homomorphism from G into the multiplicative group of integers mod p, we have

$$|G : H| \leqslant p - 1. \tag{16}$$

Also,

$$i * \sigma = i \quad \text{and} \quad \sigma(v\varepsilon^i) = v\varepsilon^i \quad \text{for all } \sigma \in H, \tag{17}$$

since $i * \sigma \equiv ir(\sigma) + t(\sigma) = i \pmod{p}$ when $\sigma \in H$.

For $0 \leqslant i < p$, write $s_i = |S(h_i)|$ and let $T = \{i | s_i > 0\}$. Note that $i \in T$ iff $\gamma_i \neq 0$ and, in fact, no subsum of h_i is zero for $i \in T$. By (14), x does not vanish on G and thus $|T| > p/2 > 1$. Since $\Sigma s_i = s$, it follows that all $s_i < s$ and thus the inductive hypothesis yields

$$\left|G\left(v\varepsilon^i h_i\right)\right| \leqslant 2^{s_i - 1} \quad \text{for } i \in T. \tag{18}$$

For $i \in T$, let π_i denote the restriction homomorphism $H \to \mathrm{Gal}(\mathbf{Q}(v\varepsilon^i h_i)/\mathbf{Q})$. Since the fields $\mathbf{Q}(v\varepsilon^i h_i)$ for $i \in T$ generate $\mathbf{Q}(f)$, we have

$\bigcap_{i\in T}\ker \pi_i = 1$. Therefore, if $K \subseteq H$ is any subgroup, we conclude that

$$|K| \leqslant \prod_{i\in T} |\pi_i(K)|. \tag{19}$$

Suppose $\gamma_j = 0$ for some j. Then (12) and (17) yield $x(\sigma) = 0$ for all $\sigma \in H$, and hence by (13), H fixes all $v\varepsilon^i\gamma_i$. Therefore, $\pi_i(H) \subseteq G(v\varepsilon^i h_i)$. Now (16), (18) and (19) yield

$$|G| \leqslant (p-1)\prod_{i\in T} 2^{s_i-1} = (p-1)2^{s-|T|}$$

and it suffices to show that $(p-1) \leqslant 2^{|T|-1}$. Since $|T| > p/2$, the result follows in this case.

Assume now that all $\gamma_i \neq 0$ so that $T = \{0, 1, \ldots, p-1\}$. Since $p > s/2$, there must exist some j with $s_j = 1$ and we fix such a j. It is not the case that γ_j is equal to a subsum of h_i for every i since otherwise we could decompose $h_i = h_i' \dotplus h_i''$ with $\Sigma(h_i') = \gamma_j$ for each i, and then

$$f' = v\big(h_0' \dotplus \varepsilon h_1' \dotplus \cdots \dotplus \varepsilon^{p-1}h_{p-1}'\big)$$

would yield a zero subsum for f. Choose j' such that γ_j is not a subsum of $h_{j'}$ and define $l \in \mathcal{F}$ by

$$l(u) = h_{j'}(u) - h_j(u) \quad \text{for } u \in U.$$

Since $|S(h_j)| = 1$, it follows that l has no zero subsum. Also

$$S(h_j) \cup S(h_{j'}) = S(l) \tag{20}$$

and

$$|S(l)| \leqslant 1 + s_{j'} < s \tag{21}$$

where the latter inequality holds since $p > 2$ and all $s_i > 0$.

By (12) and (17), H fixes all $\gamma_i - \gamma_j$ and, in particular, H fixes $\Sigma(l) = \gamma_{j'} - \gamma_j$. Let K be the kernel of the restriction map π: $H \to \mathrm{Gal}(\mathbf{Q}(l)/\mathbf{Q})$. Then $\pi(H) \subseteq G(l)$ and

$$|H : K| = |\pi(H)| \leqslant |G(l)| \leqslant 2^{s_{j'}} \tag{22}$$

by (21) and the inductive hypothesis.

Since $\gamma_j \in \mathbf{Q}(h_j) \subseteq \mathbf{Q}(l)$ by (20), we see that K fixes γ_j and thus x vanishes on K by (12) and (17). By (13) then, $\pi_i(K) \subseteq G(v\varepsilon^i h_i)$ for all i. Since K fixes $v\varepsilon^{j'}$ by (17), and fixes all elements of $S(h_{j'})$ by (20), we have $\pi_{j'}(K) = 1$. Now (18) and (19) yield

$$|K| \leqslant \prod_{i\neq j'} 2^{s_i-1} = 2^{s-s_{j'}-p+1}.$$

Combining this with (22) and (16), we obtain

$$|G| \leqslant (p-1)2^{-(p-2)}2^{s-1} \leqslant 2^{s-1}.$$

This proves (b) for primitive $f \in \mathcal{F}$.

Now suppose that $f \in \mathcal{F}$ is imprimitive and has no zero subsum. Write $f = f_1 \dotplus \cdots \dotplus f_r$ where $S(f_i) \neq \emptyset$, $r \geqslant 2$, and $G = G(f)$ permutes the $\Sigma(f_i)$. Let $\hat{H} = \{\sigma \in G \mid \sigma(\Sigma(f_i)) = \Sigma(f_i) \text{ for all } i\}$. Then $G/\hat{H}$ is isomorphic to an abelian subgroup of the symmetric group on r symbols and, hence,

$$|G : \hat{H}| \leqslant [3^{r/3}] \tag{23}$$

by [1]. Let $\hat{\pi}_i \colon \hat{H} \to \mathrm{Gal}(\mathbf{Q}(f_i)/\mathbf{Q})$ be the restriction map. Then $\hat{\pi}_i(\hat{H}) \subseteq G(f_i)$ and, reasoning as above, we obtain

$$|\hat{H}| \leqslant \prod_{i=1}^{r} |G(f_i)| \leqslant 2^{s-r}.$$

By (23),

$$|G| \leqslant [3^{r/3}]2^{s-r} \leqslant 2^{s-1}.$$

This completes the proof. □

3. **Rational polygons.** If Π is an n-gon in the complex plane, we can view Π as a vector diagram showing that a certain sum of n complex numbers is zero. Suppose that all sides and angles of Π are rational (where angles are measured in degrees). After a suitable rotation, the sides of Π correspond to positive rational multiples of roots of unity and we have an expression of the form $\sum_{i=1}^{n} a_i\varepsilon_i = 0$ with $\varepsilon_i \in U$ and $a_i \in \mathbf{Q}$, $a_i > 0$.

For simplicity, we shall consider only convex n-gons Π whose interior angles are all less than 180°. Then all ε_i are distinct and in the notation of §2 we have $\Sigma(f) = 0$ where $f \in \mathcal{F}$ is defined by $S(f) = \{\varepsilon_i\}$ and $f(\varepsilon_i) = a_i$. We mention that Π has a pair of parallel sides iff $\varepsilon_i = -\varepsilon_j$ for some i, j. Also, note that rotation of Π through a rational angle is equivalent to the replacement of f by uf for some $u \in U$.

If $h = h_1 \dotplus h_2 \in \mathcal{F}$ with $S(h_i) \neq 0$, we shall say that each $\Sigma(h_i)$ is a *proper* subsum of h. Note that if f corresponds to Π as above and $n \leqslant 5$, then f has a zero proper subsum iff Π has a pair of equal and parallel sides.

THEOREM 3.1. *Let $f \in \mathcal{F}$ with $\Sigma(f) = 0$ and assume that all proper subsums of f are nonzero. Let $s = |S(f)|$. Then there exist $v \in U$ and $g \in \mathcal{F}$ such that $f = vg$ and $k(g)$ divides $\prod_{p \leqslant s} p$ where p runs over primes. In addition, if s is prime and $f(u) \geqslant 0$ for all u, then either $s \nmid k(g)$ or else $k(g) = s$ and g is constant on U_s.*

Before proving the theorem, we mention some applications to rational n-gons with $n \leqslant 5$. Results for $n \geqslant 6$ are more complicated to state and we omit them.

COROLLARY 3.2. *Let* Π *be a convex n-gon (with interior angles less than* 180°*). Let* $n \leq 5$ *and assume that all sides and angles of* Π *are rational. Then one of the following occurs*:

(a) Π *is a regular pentagon.*

(b) Π *has a pair of equal and parallel sides.*

(c) *All angles of* Π *lie in* $\{60°, 120°\}$.

PROOF. As in the first two paragraphs of this section, Π yields some $f \in \mathcal{F}$ with $|S(f)| \leq 5, f(u) \geq 0$ for all $u \in U$ and $\Sigma(f) = 0$. If f has a zero proper subsum, then (b) occurs. Assume this is not the case. By Theorem 3.1, therefore, we may assume (by rotating Π so that $f = g$) that $k(f)$ divides $2 \cdot 3 \cdot 5$.

If $5 \nmid k(f)$, then $S(f) \subseteq U_6$ and (c) follows. Suppose $5 | k(f)$. Then the theorem yields that $S(f) = U_5$ and f is constant on U_5. In this case, (a) holds. □

As an easy consequence of Corollary 3.2, we mention the following.

COROLLARY 3.3. *Let* Π *be a convex n-gon with* $n \leq 5$ *and all sides and angles rational. Suppose that no two sides of* Π *are parallel. Then either* Π *is an equilateral triangle or it is a regular pentagon.*

PROOF OF THEOREM 3.1. Choose $u \in U$ so that $k(uf)$ is as small as possible and write $g = uf$. Let $k = k(g)$ and write $k = p^a m$ where p is prime, $a \geq 1$ and $p \nmid m$. Let δ be a primitive p^ath root of unity.

First assume $a > 1$ and write $q = p^{a-1}$ and

$$g = h_0 \dotplus \delta h_1 \dotplus \cdots \dotplus \delta^{q-1} h_{q-1}$$

with $S(h_i) \subseteq U_{mp}$. Since $1, \delta, \ldots, \delta^{q-1}$ are linearly independent over $\mathbf{Q}_{mp}$ and $\Sigma(g) = 0$, we have $\Sigma(h_i) = 0$ for all i. Since g has no zero proper subsum, we must have $g = \delta^i h_i$ for some i. Since

$$k(h_i) \leq mp < mp^a = k(g),$$

this contradicts the choice g and we conclude that $a = 1$.

Now write

$$g = h_0 \dotplus \delta h_1 \dotplus \cdots \dotplus \delta^{p-1} h_{p-1}$$

with $S(h_i) \subseteq U_m$. Since $1, \delta, \delta^2, \ldots, \delta^{p-2}$ are linearly independent over $\mathbf{Q}_m$ and $\sum_{i=0}^{p-1} \delta^i = 0$, we conclude from $\Sigma(g) = 0$ that all $\Sigma(h_i)$ are equal, say to γ. If $\gamma = 0$, then the condition that g has no zero proper subsum forces $g = \delta^i h_i$ for some i and this yields a contradiction as above since $k(h_i) < k(g)$.

It follows that $\gamma \neq 0$ and thus $S(h_i) \neq \varnothing$ for all i. In particular, this forces $p \leq s$.

To prove the final assertion, suppose $s = p$ and that $g(x) \geq 0$ for all $x \in U$. We have then $|S(h_i)| = 1$ and we write $S(h_i) = \{\varepsilon_i\}$. Now $h_i(\varepsilon_i) \geq 0$

and $\varepsilon_i h_i(\varepsilon_i) = \gamma$. This forces all ε_i to be equal, say to ε. Then ε is a primitive mth root of unity and $g = \varepsilon g_0$ where $S(g_0) \subseteq U_p$. The minimality of $k(g)$ forces $m = 1$ and hence $\varepsilon = 1$, $S(g) = U_p$ and g has the constant value γ on U_p. □

We give one further corollary.

COROLLARY 3.4. *A triangle with rational angles and two rational sides is either isosceles or else is a* 30°-60°-90° *triangle.*

PROOF. Let triangle ABC have rational angles and assume that sides AB and AC are rational. If $\angle B > 90°$, reflect side AB about the altitude drawn from A so as to obtain a new triangle $AB'C$ which also satisfies the hypotheses. We may thus assume that $\angle B \leqslant 90°$ and $\angle C < 90°$.

Now reflect the triangle about BC so as to obtain the figure $BACA'$. If $\angle B = 90°$, this figure is the triangle ACA' and is equilateral by Corollary 3.3. This yields $\angle A = 60°$ and $\angle C = 30°$ as desired.

Suppose $\angle B < 90°$. Then $BACA'$ is a convex quadrilateral and has a pair of parallel sides by Corollary 3.3. If, say, AB and CA' are parallel, we have $\angle ABC = \angle A'CB = \angle ACB$ and the triangle is isosceles. □

4. **Examples and remarks.** For each $s \leqslant 4$, we exhibit a primitive $f \in \mathcal{F}$ with $\Sigma(f) \neq 0$ such that $|S(f)| = s$ and $|G(f)| = 2^{s-1}$. In particular, this shows that Theorem 2.2(b) is best possible for these s. For $s = 1$ the situation is trivial. To handle the cases $s = 2, 3$ and 4, we introduce the notation $\omega = e^{2\pi i/3}$ and $\varepsilon = e^{2\pi i/5}$. We have

$$i(1 + 2\omega) = -\sqrt{3}\,, \quad i(1 + 2\varepsilon + 2\bar{\varepsilon}) = i\sqrt{5}\,,$$

$$i(-\omega - \omega^2 + 2\varepsilon + 2\bar{\varepsilon}) = i\sqrt{5}\,.$$

Each of these sums has degree 2 over $\mathbf{Q}$ and

$$|\mathbf{Q}(i, i\omega) : \mathbf{Q}| = 4, \quad |\mathbf{Q}(i, i\varepsilon) : \mathbf{Q}| = 8, \quad |\mathbf{Q}(i\omega, i\varepsilon) : \mathbf{Q}| = 16.$$

These yield the desired examples. (We omit the proof of primitivity.)

LEMMA 4.1. *Let $f \in \mathcal{F}$ with no zero subsum. Then there exists $g \in \mathcal{F}$ with no zero subsum such that*

(a) $|G(g)| \geqslant 3|G(f)|$,

(b) $|S(g)| = |S(f)| + 3$.

PROOF. Choose a prime $p \nmid k(f)$ such that $p \equiv 1 \bmod 3$ and let ε_0 be a primitive pth root of unity. Let $\sigma \in \mathrm{Gal}(\mathbf{Q}_p/\mathbf{Q})$ be of order 3 and write $\varepsilon_1 = \sigma(\varepsilon_0)$ and $\varepsilon_2 = \sigma(\varepsilon_1)$. Let $h \in \mathcal{F}$ with $S(h) = \{\varepsilon_0, \varepsilon_1, \varepsilon_2\}$ and $h(\varepsilon_i) = 1$. Let $g = f \dotplus h$. Thus (b) follows. Since $1, \varepsilon_0, \varepsilon_1, \varepsilon_2$ are linearly independent over $\mathbf{Q}(f)$, it follows that g has no zero subsum. Finally, $G(g)$ contains a

subgroup isomorphic to $G(f) \times \langle \sigma \rangle$ and so $|G(g)| \geqslant 3|G(f)|$. □

THEOREM 4.2. *Let s be a natural number. Then there exists $f \in \mathcal{F}$ with no zero subsum and such that*

(a) $|S(f)| = s$,

(b) $|G(f)| \geqslant (3^{1/3})^{s-1}$.

PROOF. We use induction on s. For $s = 1$, 2 or 3, the result follows from the examples at the beginning of the section. For $s > 3$, the result follows using Lemma 4.1 and the inductive hypothesis. □

Note that for $s > 3$, the proof of Theorem 4.2 produces examples which are not necessarily primitive. The authors conjecture that for primitive $f \in \mathcal{F}$ with $\Sigma(f) \neq 0$, a bound for $|G(f)|$ exists which is of significantly smaller order of magnitude than an exponential function of $s = |S(f)|$.

We also believe that Theorem 2.2(b) would remain true if 2^{s-1} is replaced by $C(3^{1/3})^s$ for a suitable constant C. Note, however, that an improvement of the bound on $|G(f)|$ for primitive f would not, by itself, yield an improved bound in the general case.

We close with some questions. Suppose E is an arbitrary field of characteristic zero and that $f\colon U \to E$ has finite support and no zero subsum. View U as being contained in an algebraic closure of E. Is $|E(f) : E(\Sigma(f))|$ bounded in terms of $s = |S(f)|$? Does there exist a uniform bound, independent of E?

REFERENCES

1. R. Bercov and L. Moser, *On Abelian permutation groups*, Canad. Math. Bull. **8** (1965), 627–630. MR **32** #7631.

2. G. H. Hardy and E. M. Wright, *An introduction to theory of numbers*, 4th ed., Oxford Univ. Press, London, 1960. (3rd ed., 1954. MR **16**, 673.)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SAN DIEGO, LA JOLLA, CALIFORNIA 92037

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706