SUM-PRODUCT THEOREMS IN ALGEBRAIC NUMBER FIELDS

Jean Bourgain Mei-Chu Chang

§0. Introduction.

In this paper, we are solely interested in the sum-product phenomenon in characteristic 0.

Given a finite set A of real or complex numbers, the sum-set $A+A$ (respectively, the product-set AA) is defined by $A+A=\{x+y : x,y \in A\}$ (resp. $AA=\{xy : x,y \in A\}$). It was shown by Erdős and Szemerédi [ES] that for sets of real numbers, $A+A$ and AA cannot both be small. More precisely, there is some $\delta > 0$ such that

$$|A+A| + |AA| > |A|^{1+\delta}. \tag{0.1}$$

We assume here and in the sequel the set A to be large. (A proof of (0.1) for sets of complex numbers in the spirit of [ES] was given by Chang in [C1].) In their paper, Erdős and Szemerédi put forward the conjecture that for finite subsets $A \subset \mathbb{Z}$ or $A \subset \mathbb{R}$, one has

$$|A+A| + |AA| > c_\varepsilon |A|^{2-\varepsilon} \text{ for all } \varepsilon > 0. \tag{0.2}$$

The strongest results towards (0.2) were obtained so far by J. Solymosi and the current record is the validity of (0.1) for $\delta < 1/3$, for $A \subset \mathbb{R}$ (see [So]).

In the same spirit, the following more restrictive problem was also considered in [ES].

Assume $|A+A| < K|A|$ *for some fixed constant* K. *Is it true that* $|AA| > c_\varepsilon |A|^{2-\varepsilon}$ *for all* $\varepsilon > 0$*?* (0.3)

Is there a function $\varepsilon(\delta)$ *such that* $\varepsilon(\delta) \to 0$ *as* $\delta \to 0$ *and if* $|A+A| < |A|^{1+\delta}$, *then* $|AA| > c_\varepsilon |A|^{2-\varepsilon}$ *?* (0.3')

Same as (0.3) *reversing the roles of addition and multiplication.* (0.4)

Same as (0.3′) *reversing the roles of addition and multiplication.* (0.4')

Note that a typical example of sets A satisfying (0.3) are arithmetic progressions. It was shown by Tenenbaum [T] that if $A = \{1, \dots, N\}$, then

$$\frac{N^2}{(\log N)^{\alpha+\varepsilon}} < |AA| < \frac{N^2}{(\log N)^{\alpha-\varepsilon}}$$

with

$$\alpha = 1 - \frac{\log(e \log 2)}{\log 2} = 0.086.$$

There are two proofs of (0.3). One (assuming $A \subset \mathbb{R}$) is due to Elekes [El] and is based on incidence geometry (the Szemerédi-Trotter theorem). It also yields (0.3'). The other approach to (0.3) was given in [C2] using factorization in algebraic number fields. The method from [C2] gives (0.3) for subsets $A \subset \mathbb{C}$ as well and in fact establishes more generally that if $|A + A| < K|A|$, then the ℓ-fold product set $A^\ell = \{a_1 \cdots a_\ell : a_i \in A\}$ satisfies

$$|A^\ell| > c_{\ell,\varepsilon} |A|^{\ell-\varepsilon} \text{ for all } \varepsilon > 0, \tag{0.5}$$

where ℓ is any given positive integer.

It is interesting that the contributions to (0.4) and (0.4') rely on quite different ideas (there does not appear to be symmetry when reversing the roles of addition and multiplication). Note that typical sets satisfying (0.4) are geometric progressions. Using the deep results from [ESS] on linear relations in multiplicative groups of bounded rank (depending on the subspace theorem), it was shown in [C3] that (0.4) holds. In fact, it is proven there that if $|A + A| < K|A|$ with K fixed or even $K = o(\log |A|)$, then the ℓ-fold sum-set ℓA satisfies

$$|\ell A| > c_\ell |A|^\ell.$$

Validity of (0.4') for sets $A \subset \mathbb{Z}$ was established in [BC]. Because the argument from [BC] depends mainly on prime factorization, it is not clear how to extend it to subsets $A \subset \mathbb{R}$. (This question remains open.) In this paper we prove (0.4') for subsets $A \subset \mathbb{C}$ consisting of algebraic numbers of bounded degree. Note that we do not require A to be contained in the same number field of bounded degree.

Theorem 11. *Let $A \subset \mathcal{O}_K$, $|A| = N$ be a finite set of algebraic integers of bounded degree d. Assume*

$$|A.A| < R|A|.$$

Then for any $B \subset A$ and $D \subset \mathbb{C}$

$$|B + D| \geq R^{-C(d,\varepsilon)} N^{-\varepsilon} |B| \ |D|^{1-\varepsilon}.$$

In particular, the sum-sets $A+A$ and more generally ℓA satisfy

$$|A+A| > R^{-C(d,s)}N^{-\varepsilon}|A|^2$$

and

$$|\ell A| > R^{-C(d,\ell,\varepsilon)}N^{-\varepsilon}|A|^{\ell}.$$

In fact, we will prove a stronger result on additive relations, which is derived from the following proposition.

Proposition 10. *Let A be as in Theorem 11. Given $q \in \mathbb{Z}_+$, $\tau > 0$, there is a constant $\Lambda = \Lambda(d,q,\tau)$ such that given any system $\big(c(x)\big)_{x\in A} \subset \mathbb{R}_+$, we have the inequality*

$$\Big[\sum_{\substack{x_1+\cdots+x_q=\\ y_1+\cdots+y_q}} c(x_1)\cdots c(x_q)\Big]^{1/2q} \le N^{\tau}R^{\Lambda}\Big[\sum_{x\in A} c(x)^2\Big]^{1/2}.$$

Let us explain the meaning of the above inequality. Assuming $A \subset \mathbb{Z}$, then the left-hand side equals

$$\Big(\int_0^1 \Big|\sum_{x\in A} c(x)e^{2\pi i x\theta}\Big|^{2q} d\theta\Big)^{\frac{1}{2q}}.$$

In other words, the "lambda-$2q$ constant" of A is at most $N^{\tau}R^{\Lambda}$. Thus Proposition 8 is the generalization of [BC] to sets of algebraic numbers of bounded degrees.

It seems reasonable to expect statements such as Proposition 8 and Theorem 11 to be true for arbitrary finite subsets A of $\mathbb{C}$ with $|A.A| < R|A|$. But at this point our method does not allow to avoid the dependence on the degree d.

The first ingredient is closely related to a result of H. Stark [St]and provides a criterion for multiplicative independence of algebraic integers.

Proposition 5. *Fix a Galois extension K_0 of $\mathbb{Q}$. Let $\xi_1,\ldots,\xi_r$ be algebraic integers satisfying the following condition*

$$[K_0(\xi_s) : K_0] = [K_0(\xi_s,\xi_{s'}) : K_0(\xi_{s'})]$$

for all $s \neq s'$. Assume further that the ξ_s are not in the set $K_0.\{$roots of unity$\}$. Then $\xi_1,\ldots,\xi_r$ are multiplicatively independent.

Stark proved this result in case $\xi_1,\ldots,\xi_r$ are the fundamental units of distinct quadratic fields and our argument is a direct adaptation of his.

Proposition 5 has the following implication on finite sets A of algebraic integers with small multiplicative doubling

$$|A.A| < R.|A|.$$

Proposition 6. *Let A be a set of algebraic integers of bounded degree d. Assume*

$$|A.A| < R.|A|.$$

Then there is an extension field K of $\mathbb{Q}$ such that $[K : \mathbb{Q}] < C(d)$ and $|A \cap K| > (R. \log |A|)^{-C(d)}|A|$.

The next ingredient is the finiteness result from [ESS] for solutions of linear equations in multiplicative groups of finite rank, already mentioned above. But here it will just be applied in the unit group of an extension field of $\mathbb{Q}$ of bounded degree (which is a more modest result than [ESS]).

Let us point out that if we assume $A \subset K$ (an extension field of $\mathbb{Q}$) is such that distinct elements of A are not conjugate (i.e. the corresponding principal ideals are different), then the argument from [BC] could be repeated verbatim. This argument is rather combinatorially involved and will not be completely reproduced here. We will only recall the main steps and statements in our more general setting. (See Lemmas 5, 7, 8, and Proposition 9.) The additional issue of the unit may then be taken care of by the subspace theorem. This is roughly how the proof of Proposition 10 goes.

Using Proposition 5, we will also prove

Proposition 14'. *Let A be a finite set of algebraic numbers of degree at most d and such that the minimal polynomial of each element of A has coefficients bounded by M. Then*

$$|A.A| > \exp\Big(- C(d)\frac{\log M}{\log\log M}\Big).|A|^2$$

and similar for multiple product sets.

The paper is concluded with an application of Proposition 8 to incidence geometry, in the spirit of results obtained in [CS].

Remark. Returning to the problem of establishing (0.4') for general finite sets $A \subset \mathbb{R}$ or $A \subset \mathbb{C}$, it was pointed out in [BC] that a proof of the Polynomial Freiman-Ruzsa Conjecture in its full strength would allow us to proceed as in [C3] and proof the assertion. The role of the Polynomial Freiman-Ruzsa Conjecture is to reduce the rank (of the multiplicative group generated by a large subset of A) to logarithmic size, so that [ESS] becomes applicable. (See [BC2] for details.)

§1. Proof of Proposition 5.

Let p be a prime and let K be an extension of $\mathbb{Q}$ with p-th primitive root of unity

$$\omega_p = e^{\frac{2\pi i}{p}} \in K.$$

Our arguments are closely related to some techniques in [St].

Lemma 1. *If $\alpha \in K$ and $\alpha^{1/p} \notin K$, then the polynomial $x^p - \alpha$ is irreducible over K and $[K(\alpha^{1/p}) : K] = p$.*

Proof. Assume the contrary that $f(x)$, the irreducible polynomial of $\alpha^{1/p}$ is a nontrivial factor of $x^p - \alpha$. Then the roots of $f(x)$ form a proper subset of $\{\alpha^{1/p}\omega_p, \cdots, \alpha^{1/p}\omega_p^p\}$. Hence, taking their product gives $\alpha^{r/p}\omega_p^k \in K$ for some $k \in \mathbb{Z}$ with $r < p$. Therefore, $\alpha^{r/p} \in K$ implies $\alpha^{1/p} \in K$, since $(r, p) = 1$. $\square$

Lemma 2. *Assume $\alpha^{1/p} \in K(\xi_1^{1/p}, \ldots, \xi_r^{1/p})$, with $\alpha, \xi_1, \ldots, \xi_r \in K$. Then there exist $m_1, \ldots, m_r \in \mathbb{N}$ and $\gamma \in K$ such that*

$$\alpha^{1/p} = \xi_1^{m_1/p} \ldots \xi_r^{m_r/p}\gamma. \tag{2.0}$$

Proof. We may clearly assume

$$\xi_i^{1/p} \notin K\big(\xi_j^{1/p} : j \neq i\big). \tag{2.1}$$

Proceed by induction on r.

From assumption

$$\alpha^{1/p} = \sum_{k=m}^{p-1} b_k \xi_r^{k/p} \text{ with } b_k \in K_{r-1} = K(\xi_1^{1/p}, \ldots, \xi_{r-1}^{1/p}) \text{ and } b_m \neq 0.$$

Let

$$\beta^{1/p} = \frac{\alpha^{1/p}}{\xi_r^{m/p}} = b_m + b_{m+1}\xi_r^{1/p} + \cdots + b_{p-1}\xi_r^{\frac{p-1-m}{p}}. \tag{2.2}$$

If $\beta^{1/p} \in K_{r-1}$, the induction hypothesis applies and $\beta^{1/p}$ has the form $\beta^{1/p} = \xi_1^{\frac{m_1}{p}} \cdots \xi_{r-1}^{\frac{m_{r-1}}{p}} \gamma$ for some $\gamma \in K$. Hence (2.0) holds. Otherwise, from Lemma 1, it follows that $x^p - \beta$ is irreducible over K_{r-1}. Let $Tr = Tr_{K_r/K_{r-1}}$. Then $Tr(\beta^{1/p}) = 0$ and by (2.2)

$$0 = b_m Tr(1) + \sum_{p>k>m} b_k Tr(\xi_r^{\frac{k-m}{p}}). \tag{2.3}$$

Since $\xi_r^{1/p} \notin K_{r-1}$ by (2.1), also $\xi_r^{\frac{k-m}{p}} \notin K_{r-1}$ for $0 \leq m < k < p$. By Lemma 1, $x^p - \xi_r^{k-m}$ is irreducible over K_{r-1}, hence $Tr(\xi_r^{\frac{k-m}{p}}) = 0$. It follows from (2.3) that

$$0 = b_m Tr(1),$$

hence $b_m = 0$, which is a contradiction. This proves Lemma 2. $\square$

Lemma 3. *Let K be Galois over $\mathbb{Q}$, and let $\alpha, \xi_1, \dots, \xi_r \in K$. For $K_0 < K$, we denote $K_r = K_0(\xi_1, \dots, \xi_r)$. Assume that*

$$d := [K_0(\alpha) : K_0] = [K_r(\alpha) : K_r] < p. \tag{3.0}$$

Then if

$$\alpha^{1/p} \in K(\xi_1^{1/p}, \dots, \xi_r^{1/p}),$$

there is $a \in K_0$ such that

$$(a\alpha)^{1/p} \in K.$$

Proof. By Lemma 2, there exists $\gamma \in K$ such that

$$\alpha = \xi_1^{m_1} \cdots \xi_r^{m_r} \gamma^p. \tag{3.1}$$

Since the minimal polynomial of α over K_0 is irreducible over K_r, the conjugates $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ of α over K_0 are also conjugates over K_r. Let $L = K_r(\alpha_1, \dots, \alpha_d)$ be the splitting field of α over K_r. Since K is Galois over over $\mathbb{Q}$ (hence over K_r) and $\alpha \in K$, we have $L \subset K$. Hence there are automorphisms

$$\sigma_i \in \ \mathrm{Aut}_{K_r} L,$$

such that

$$\sigma_i(\alpha) = \alpha_i.$$

Hence each σ_i has an extension $\tilde{\sigma}_i \in \mathrm{Aut}_{K_r} K$.

By (3.1)

$$\prod_{i=1}^{d} \alpha_i = (\xi_1^{m_1} \cdots \xi_r^{m_r})^d \ \prod_{i=1}^{d} \tilde{\sigma}_i(\gamma)^p. \tag{3.2}$$

Let

$$a = \prod_{i=1}^{d} \alpha_i \in K_0.$$

From (3.1) and (3.2),

$$\alpha^d = (\xi_1^{m_1} \cdots \xi_r^{m_r})^d \gamma^{dp} = a\Big(\prod_{i=1}^{d} \frac{\gamma}{\tilde{\sigma}_i(\gamma)} \Big)^p =: a\gamma_1^p, \tag{3.3}$$

where $\gamma_1 \in K$. Write $1 = ud + vp$ for some $u, v \in \mathbb{Z}$, since $(d, p) = 1$. From (3.3), $\alpha = a^u(\gamma_1^u \alpha^v)^p$ and hence $(a^{-u}\alpha)^{1/p} \in K$. This proves Lemma 3. $\square$

Lemma 3′. *Let K be Galois over $\mathbb{Q}$ and let $K_0 < K$. Suppose $\mathcal{C} = \{\xi_1, \dots, \xi_r\} \subset K$ is a set of conjugates over K_0 with $r < p$. Let $\alpha \in K$, satisfying*

$$[K_0(\alpha) : K_0] = [K_0(\alpha, \xi_1) : K_0(\xi_1)]. \tag{3.4}$$

Then if

$$\alpha^{1/p} \in K(\xi_1^{1/p}, \dots, \xi_r^{1/p}),$$

there is $a \in K_0$ such that

$$(a\alpha)^{1/p} \in K.$$

Proof. By Lemma 2, there is $\gamma \in K$ such that

$$\alpha = \xi_1^{m_1} \cdots \xi_r^{m_r} \gamma^p. \tag{3.5}$$

Assumption (3.4) is equivalent to

$$[K_0(\xi_1) : K_0] = [K_0(\alpha, \xi_1) : K_0(\alpha)]$$

and since $\xi_1, \dots, \xi_r$ are conjugates over K_0, also

$$[K_0(\xi_s) : K_0] = [K_0(\alpha, \xi_s) : K_0(\alpha)], \text{ for } 1 \le s \le r.$$

For all s, the map

$$\varphi : K_0(\alpha)(\xi_1) \to K_0(\alpha)(\xi_s)$$

which is identity on $K_0(\alpha)$ and sends ξ_1 to ξ_s is an isomorphism. Denote $G = \mathrm{Aut}_{K_0(\alpha)} K_0(\alpha, \xi_1, \dots, \xi_r)$. Let $\tilde{\varphi} \in G$ be the extension of φ to $K_0(\alpha, \xi_1, \dots, \xi_r)$. Hence G acts transitively on $\{\xi_1, \dots, \xi_r\}$. For $\tau \in G$ let $\tilde{\tau}$ be its extension in $\mathrm{Aut}_{K_0(\alpha)} K$.

Returning to (3.5)

$$\alpha^{|G|} = \prod_{\tau \in G} \tau(\xi_1)^{m_1} \cdots \prod_{\tau \in G} \tau(\xi_r)^{m_r} \Big(\prod_{\tau \in G} \tilde{\tau}(\gamma) \Big)^p. \tag{3.6}$$

Since G acts transitively on $\{\xi_1, \dots, \xi_r\}$, we have

$$\prod_{\tau \in G} \tau(\xi_1) = \cdots = \prod_{\tau \in G} \tau(\xi_r)$$

$$\prod_{\tau \in G} \tau(\xi_1)^r = \prod_{\tau \in G} \tau(\xi_1 \dots \xi_r) = N_{K_0(\xi_1)/K_0}(\xi_1)^{|G|} \in K_0.$$

Therefore

$$\alpha^{r|G|} = a\gamma_1^p \text{ with } a \in K_0, \gamma_1 \in K.$$

Since $|G|$ divides $r!$ and $p > r$, the conclusion follows as in Lemma 3. □

Notation. For a set S, $S^{1/n} := \{s^{1/n} : s \in S\}$.

For an extension K of $\mathbb{Q}$, we denote the ring of algebraic integers of K by $\mathcal{O}_K$.

Lemma 4. *Let K_0 be Galois over $\mathbb{Q}$. Let $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_r$ be systems of conjugate algebraic integers over $\mathcal{O}_{K_0}$ such that for ξ, ξ' from different systems*

$$[K_0(\xi') : K_0] = [K_0(\xi, \xi') : K_0(\xi)]. \tag{4.0}$$

Then, taking p a sufficiently large prime and defining

$$K_{(s)} = K_0\Big(\omega_p, \bigcup_{i \le s} \mathcal{C}_i^{1/p}, \bigcup_{i > s} \mathcal{C}_i\Big) \tag{4.1}$$

we have

$$\xi^{1/p} \notin K_{(s)}, \ \textit{for } \xi \in \mathcal{C}_i, i > s \tag{4.2}$$

unless

$$\xi \in K_0 \ \{\textit{roots of unity}\}. \tag{4.3}$$

Proof. We proceed by reduction on s.

Thus first, we need to show that if $\xi \in \bigcup_{1 \le s \le r} \mathcal{C}_s$ and (4.3) fails then

$$\xi^{1/p} \notin K_{(0)} = K_0\Big(\omega_p, \bigcup_{1 \le s \le r} \mathcal{C}_s\Big). \tag{4.4}$$

Assume $\xi^{1/p} \in K_{(0)}$. Then

$$\xi = \gamma^p \text{ for some } \gamma \in K_{(0)}. \tag{4.5}$$

Claim. $\xi = \lambda^p$, *for some algebraic integer* $\lambda \in \mathcal{O}_{K_0(\xi)}$.

Proof of Claim.

Since ξ is an algebraic integer, by (4.5), γ is an algebraic integer over $\mathcal{O}_{K_0(\xi)}$. Again, by (4.5),

$$\xi^{[K_{(0)} : K_0(\xi)]} = N_{K_{(0)}/K_0(\xi)}(\xi) = \big(N_{K_{(0)}/K_0(\xi)}(\gamma)\big)^p, \tag{4.6}$$

where

$$[K_{(0)} : K_0(\xi)] \ \Big| \ [K_{(0)} : K_0] = [K_{(0)} : K_0(\omega_p)] \, [K_0(\omega_p) : K_0]. \tag{4.7}$$

By (4.4), $K_{(0)}$ is obtained from $K_0(\omega_p)$ by a sequence of extensions, where elements of $\bigcup \mathcal{C}_s$ are added consecutively. Hence certainly

$$[K_{(0)} : K_0(\omega_p)] \le (d!)^r \tag{4.8}$$

where $d = \max_{\xi \in \cup \mathcal{C}_s} [\mathbb{Q}(\xi) : \mathbb{Q}] < p$ for p chosen large enough.

Also $[K_0(\omega_p) : K_0] \leq [\mathbb{Q}(\omega_p) : \mathbb{Q}] = p - 1$. By (4.7) and (4.8), we see that

$$([K_{(0)} : K_0(\xi)], p) = 1. \tag{4.9}$$

The Claim follows from (4.6), (4.9) and that $N_{K_{(0)}/K_0(\xi)}(\gamma) \in \mathcal{O}_{K_0(\xi)}$.

Therefore

$$N_{K_0(\xi)/\mathbb{Q}}(\xi) = [N_{K_0(\xi)/\mathbb{Q}}(\lambda)]^p.$$

Since both $N_{K_0(\xi)/\mathbb{Q}}(\xi)$ and $N_{K_0(\xi)/\mathbb{Q}}(\lambda)$ are integers, choosing p large enough, this may happen only if $N_{K_0(\xi)/\mathbb{Q}}(\xi) = \pm 1$. Hence ξ and λ are units. Since ξ is not a root of unity, representation of ξ and λ in the unit group of $K_0(\xi)$ as product of a root of unity and fundamental units, shows that (4.5) cannot hold if p is taken large enough.

Next we perform the inductive step $s - 1$ implying s.

Clearly we may take $i = s + 1$. Thus assume that

$$\xi \in \mathcal{C}_{s+1} \text{ and } \xi^{1/p} \in K_{(s)} = K_{(s-1)}(\mathcal{C}_s^{1/p}).$$

Notice that by construction $K_{(s-1)}$ is a Galois extension of $\mathbb{Q}$. Apply Lemma $3'$ with $K = K_{(s-1)}$ and $\alpha = \xi$. Thus there exists $a \in K_0$

$$(a\xi)^{1/p} \in K_{(s-1)}. \tag{4.10}$$

Replace $\mathcal{C}_{s+1}$ by $a.\mathcal{C}_{s+1}$ (the other $\mathcal{C}_i$ remain). The fields $K_{(i)}$ remain the same for $i \leq s$. From the induction hypothesis at stage $s - 1$ and (4.10), we get that

$$a\xi \in K_0 \ \{\text{root of unity}\}.$$

Hence (4.3) holds. This proves Lemma 4. □

Proposition 5. *Let K_0 be Galois over $\mathbb{Q}$ and let $\xi_1, \xi_2, \ldots, \xi_r$ be algebraic integers not of the form K_0 $\{$roots of unity$\}$ satisfying*

$$[K_0(\xi_s) : K_0] = [K_0(\xi_s, \xi_{s'}) : K_0(\xi_{s'})],$$

for all $1 \leq s \neq s' \leq r$. Then $\xi_1, \ldots, \xi_r$ are multiplicatively independent.

Proof. Let $\mathcal{C}_s$ be the set of conjugates of ξ_s over K_0. Condition (4.0) clearly holds. Apply Lemma 4 with suitable p.

Since $\xi_{s+1}^{1/p} \notin K_{(s)}$, it follows from (4.1) that

$$\xi_{s+1}^{1/p} \neq \xi_1^{m_1/p} \dots \xi_s^{m_s/p} \xi_{s+1}^{m'_{s+1}};$$

i.e.,

$$\xi_1^{m_1} \dots \xi_s^{m_s} \xi_{s+1}^{p\, m'_{s+1}-1} \neq 1 \tag{5.1}$$

for any $m_1, \dots, m'_{s+1} \in \mathbb{Z}$, p large enough. If $\xi_1, \dots, \xi_r$ are multiplicatively dependent, there are $\nu_1, \dots, \nu_s$ and $\nu_{1+1} \in \mathbb{Z}$, $\nu_{s+1} \neq 0$ such that

$$\xi_1^{\nu_1} \dots \xi_s^{\nu_s} \xi_{s+1}^{\nu_{s+1}} = 1. \tag{5.2}$$

Take $p > \nu_{s+1}$ and $q \in \mathbb{Z}$ such that

$$q\nu_{s+1} \equiv -1 \qquad (\mathrm{mod}\ p).$$

Putting

$$m_1 = \nu_1 q, \dots, m_s = \nu_s q, m'_{s+1} p - 1 = q\nu_{s+1}, \tag{5.3}$$

we get a contradiction. $\square$

§2. Consequences.

We first establish the following proposition.

Proposition 6. *Let A be a set of algebraic integers of degree bounded by d. Assume*

$$|AA| < R\,|A|. \tag{6.1}$$

Then there is an extension $K > \mathbb{Q}$ satisfying

$$[K : \mathbb{Q}] < C(d) \tag{6.2}$$

and

$$|A \cap K| > (R \log |A|)^{-C(d)} |A|. \tag{6.3}$$

Proof.

In Lemma 4, take $K_0 = \mathbb{Q}$ and denote for $\xi \in A$ by $\mathcal{C}(\xi)$ the set of conjugates of ξ. Let $\xi_1, \dots, \xi_r \in A \setminus \mathbb{Q}$ {roots of unity} be a maximal set of elements such that $\mathcal{C}_1 = \mathcal{C}(\xi_1), \dots, \mathcal{C}_r = \mathcal{C}(\xi_r)$ satisfy (4.0).

Note that by the degree assumption

$$A \cap \mathbb{Q}\{\text{roots of unity}\} \subset \mathbb{Q}\big(\omega_q, q \le C(d)\big) =: L$$

where, denoting by $C(d)$ various constants depending on d

$$[L : \mathbb{Q}] < C(d).$$

We may therefore assume that $|A\backslash L| > \frac{1}{2}|A|$, since otherwise (6.3) holds with $K = L$. It follows from the maximality that if $\xi \in A\backslash L$, then for some $s = 1, \dots, r$ we have

$$\begin{aligned}[\mathbb{Q}(\mathcal{C}_s, \xi) : \mathbb{Q}(\mathcal{C}_s)] \le & [\mathbb{Q}(\xi_s, \xi) : \mathbb{Q}(\xi_s)] \\ \le & [\mathbb{Q}(\xi) : \mathbb{Q}] - 1 \le d - 1. \end{aligned} \tag{6.4}$$

We establish a bound on r using the property that $\xi_1, \dots, \xi_r$ are multiplicatively independent together with (6.1). Denoting $A_1 = \{\xi_1, \dots, \xi_r\}$, it follows from the Plunnecke-Ruzsa inequality that for arbitrary $\ell \in \mathbb{Z}_+$

$$\binom{r}{\ell} < |\underbrace{A_1 \dots A_1}_{\ell}| = |A_1^\ell| \le |A^\ell| \le R^{\ell+1}|A|. \tag{6.5}$$

Hence, for $\ell < \frac{r}{2}$, we find

$$r < 2\ell R^{1+\frac{1}{\ell}} |A|^{\frac{1}{\ell}} \tag{6.6}$$

implying for $\ell = [\log |A|]$

$$r < 2e^2 R \log |A|. \tag{6.7}$$

From the preceding, we may specify some $s_1 = 1, \dots, r$ and a subset $A^{(1)} \subset A\backslash L$ satisfying

$$|A^{(1)}| > \frac{1}{r}\frac{|A|}{2} \tag{6.8}$$

and for $\xi \in A^{(1)}$

$$[\mathbb{Q}(\mathcal{C}_{s_1})(\xi) : \mathbb{Q}(\mathcal{C}_{s_1})] \le d - 1. \tag{6.9}$$

Take now $K_0 = \mathbb{Q}(\mathcal{C}_{s_1})$. Then

$$[K_0 : \mathbb{Q}] \le C(d) \tag{6.10}$$

and

$$[K_0(\xi) : K_0] \le d - 1 \text{ for any } \xi \in A^{(1)}. \tag{6.11}$$

Repeat the preceding considering now the system $\{\mathcal{C}(\xi) : \xi \in A^{(1)}\}$ and $\mathcal{C}(\xi)$ the conjugates of ξ over K_0, Clearly, by (6.10), again

$$A_1 \cap K_0\{\text{roots of unity}\} \subset K_0(\omega_q, q \le C(d)) =: L_1$$

where

$$[L_1 : \mathbb{Q}] < C(d).$$

By (6.7) and (6.8),

$$|A^{(1)}| > C\frac{|A|}{R\log|A|}. \tag{6.12}$$

We may assume

$$|A^{(1)}\backslash L_1| > \frac{1}{2}|A^{(1)}|,$$

since otherwise (6.3) holds with $K = L_1$.

The same bound (6.7) on r holds. This gives $A^{(2)} \subset A^{(1)}\backslash L_1$ such that for some s_2

$$|A^{(2)}| > \frac{1}{2r}|A^{(1)}|,$$

and for $\xi \in A^{(2)}$

$$\begin{aligned}[K_0(\mathcal{C}_{s_2})(\xi) : K_0(\mathcal{C}_{s_2})] \leq & [K_0(\xi) : K_0] - 1 \\ \leq & d - 2.\end{aligned} \tag{6.13}$$

Redefine K_0 as $K_0(\mathcal{C}_{s_2})$ and start over again.

Since the process has to terminate after at most d iterations, the conclusion is clear. This proves Proposition 6. $\square$

We now focus on Proposition 10. First, we need a preliminary result. (Lemma 7 below.)

Fix a prime ideal $\mathcal{P}$ of $\mathcal{O}_K$.

Notation. For $x \in \mathcal{O}_K$, denote $m(x) = \max\{m \in \mathbb{N} : x \in \mathcal{P}^m\}$.

Note that $x \in \mathcal{P}^m$ is equivalent to $\mathcal{P}^m|(x)$.

The following is an analogue of Proposition 6 in [C].

Lemma 7. *For $q = 2^k \in \mathbb{Z}_+$ and $c : \mathcal{O}_K \to \mathbb{R}_+$, we have*

$$\begin{aligned}&\Big[\sum_{x_1+\cdots+x_q=y_1+\cdots+y_q} c(x_1)\cdots c(x_q)c(y_1)\cdots c(y_q)\Big]^{1/2q} \\ \leq & c(q)\Big\{\sum_{m=0}^{\infty}\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q \\ m(x_1)=\cdots=m(y_q)=m}} c(x_1)\cdots c(x_q)c(y_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2}.\end{aligned} \tag{7.1}$$

Proof. Here we only treat the case $q = 2$, since the general case is similar.

If $x_1 + x_2 = y_1 + y_2$ and $m = \min_i\{m(x_i), m(y_i)\}$, then clearly m has to appear at least twice. Indeed, if $m = m(x_1) < m' = \min\{m(x_2), m(y_1), m(y_2)\}$, then $\mathcal{P}^{m'}$ divides $(y_1 + y_2 - x_2)$ but not (x_1), a contradiction.

Therefore

$$\sum_{x_1+x_1=y_1+y_2} c(x_1)c(x_2)c(y_1)c(y_2) \tag{7.2}$$

$$\lesssim \sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(x_2)\\ x_1+x_2=z}} c(x_1)c(x_2)\Big]\Big[\sum_{y_1+y_2=z} c(y_1)c(y_2)\Big] \tag{7.3}$$

$$+ \sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(y_1)\\ x_1-y_1=z}} c(x_1)c(y_1)\Big]\Big[\sum_{y_2-x_2=z} c(x_2)c(y_2)\Big] \tag{7.4}$$

Estimate (7.3) (similarly for (7.4)) by Cauchy-Schwarz. We obtain

$$(7.3) \le \Big\{ \sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(x_2)\\ x_1+x_2=z}} c(x_1)c(x_2)\Big]^2\Big\}^{1/2} \cdot (7.2)^{1/2}$$

and

$$(7.4) \le \Big\{ \sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(y_1)\\ x_1-y_1=z}} c(x_1)c(y_1)\Big]^2\Big\}^{1/2} \cdot (7.2)^{1/2}.$$

The triangle inequality gives

$$\sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(x_2)\\ x_1+x_2=z}} c(x_1)c(x_2)\Big]^2$$

$$\le \Big\{ \sum_{m=0}^{\infty} \Big(\sum_{z\in\mathcal{O}_K} \Big[\sum_{\substack{m(x_1)=m(x_2)=m\\ x_1+x_2=z}} c(x_1)c(x_2)\Big]^2\Big)^{1/2}\Big\}^2$$

$$= \Big\{ \sum_{m=0}^{\infty} \Big[\sum_{\substack{x_1+x_2=y_1+y_2\\ m(x_1)=\cdots=m(y_2)=m}} c(x_1)c(x_2)c(y_1)c(y_2)\Big]^{1/2}\Big\}^2 = (7.1)^4. \tag{7.5}$$

Hence

$$(7.2) \lesssim (7.3) + (7.4) \lesssim (7.1)^2 \cdot (7.2)^{1/2}$$

and we prove the case of $q = 2$. $\square$

Using Lemma 7 as basic ingredient, one may then establish the analogue of Proposition 3 in [BC], relying on a similar multiscale argument. The only difference from [BC] is that here we invoke factorization in prime ideals rather than rational primes. If in particular we take in [BC], Proposition 3, $A_1 = A_2, \mathcal{G} = A_1 \times A_2$, we conclude the following:

Proposition 8. *Let $\mathcal{A}$ be a finite set of ideals in $\mathcal{O}_K$, $|\mathcal{A}| = N$, such that*

$$|\mathcal{A}.\mathcal{A}| < K|\mathcal{A}|. \tag{8.1}$$

Let $q \in \mathbb{Z}_+, \tau > 0$ be fixed. There is a subset $\mathcal{A}' \subset \mathcal{A}$ satisfying

(i). $|\mathcal{A}'| > N^{-\tau}|\mathcal{A}|$

(ii). Let $B \subset \mathcal{O}_K$ and assume that B is union

$$B = \bigcup_{I \in \mathcal{A}'} B_I,$$

where

$$B_I = \{x \in B : (x) = I.J \text{ where } J \text{ is relative prime with all ideals in } \mathcal{A}'\}.$$

Let $c(x) \in \mathbb{R}_+$ for $x \in B$.

Then

$$\begin{aligned}&\Big[\sum_{\substack{x_1+\cdots+x_q=\\ y_1+\cdots+y_q}} c(x_1)\cdots c(x_q)c(y_1)\cdots c(y_q)\Big]^{1/2q}\\ \le& N^{\tau}K^{\Lambda}\Big\{\sum_{I\in\mathcal{A}'}\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q\\ x_1,\dots,y_q\in B_I}} c(x_1)\cdots c(x_q)c(y_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2},\end{aligned} \tag{8.2}$$

where $\Lambda = \Lambda(q, \tau)$.

We may then establish

Proposition 9. *Let $A \subset \mathcal{O}_K$ be a finite set, $|A| = N$ and*

$$|A.A| < K.|A|. \tag{9.1}$$

Given $q \in \mathbb{Z}_+, \tau > 0$, there is a constant $\Lambda = \Lambda(q,\tau)$ such that if $c(x) \in \mathbb{R}_+$ for $x \in A$, we have

$$\Big[\sum_{\substack{x_1+\cdots+x_q \\ =y_1+\cdots+y_q}} c(x_1)\cdots c(y_q)\Big]^{1/2q}$$

$$\leq N^\tau K^\Lambda \Big\{ \sum_{I \text{ principal}} \Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q \\ (x_1)=\cdots=(y_q)=I}} c(x_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2}. \tag{9.2}$$

Proof.

Define

$$\mathcal{A} = \{(x) : x \in A\}.$$

Let

$$M = \max_{I \in \mathcal{A}} |\{x \in A : (x) = I\}|$$

and let

$$M = |\{x \in A : (x) = (x_0)\}|$$

for some $x_0 \in A$.

Hence

$$|A| \leq M.|\mathcal{A}|$$

and also from (9.1)

$$\begin{aligned} K^3.|A| &\geq |A.A.A| \\ &\geq |A.A.\{x \in A : (x) = (x_0)\}| \\ &\geq |\mathcal{A}.\mathcal{A}|.M. \end{aligned}$$

Hence

$$|\mathcal{A}.\mathcal{A}| < K^3|\mathcal{A}|. \tag{9.3}$$

Denote

$$\mathcal{A}_1 = \Big\{ I \in A : \quad |\{x \in A : (x) = I\}| > \frac{m}{10K}\Big\}.$$

Hence

$$|A| \leq |\mathcal{A}_1|.M + |\mathcal{A}\backslash\mathcal{A}_1|\frac{M}{10K} < |\mathcal{A}_1|.M + |\mathcal{A}|\frac{M}{10K}\ ,$$

while also

$$K.|A| \geq |A.A| > M.|\mathcal{A}|$$

and therefore

$$|\mathcal{A}_1| > \frac{|\mathcal{A}|}{2K}. \tag{9.4}$$

Apply Proposition 8 to the set $\mathcal{A}_1$ (for $\tau > 0$ specified). This gives $\mathcal{A}_1' \subset \mathcal{A}_1$ with

$$|\mathcal{A}_1'| > N^{-\tau}|\mathcal{A}_1| > \frac{|\mathcal{A}|}{2KN^{\tau}}.$$

Take

$$B = \{x \in A : \ (x) \in \mathcal{A}_1'\}.$$

Hence B satisfies

$$|B| > |\mathcal{A}_1'|.\frac{M}{10K} > \frac{|A|}{20K^2N^{\tau}} \tag{9.5}$$

and (7.7). Thus

$$\begin{aligned}&\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q\\ x_1,\dots,y_q\in B}} c(x_1)\cdots c(y_q)\Big]^{1/2q}\\ \le& N^{\tau}K^{\Lambda}\Big\{\sum_{I}\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q\\ x_1,\dots,y_q\in B\\ (x_1)=\cdots=(y_q)=I}} c(x_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2}.\end{aligned} \tag{9.6}$$

Next, write

$$\mathcal{X}_A \le \frac{1}{|B|}\sum_{z\in B^{-1}A}\mathcal{X}_{Bz},$$

where $\mathcal{X}$ denoting the indicator function. For $x \in A$,

$$c(x) \le \frac{1}{|B|}\sum_{z\in B^{-1}A} c(x)\mathcal{X}_{Bz}(x). \tag{9.7}$$

Estimate

$$\begin{aligned}
&\Big[\sum_{\substack{x_1+\cdots+x_q=\\ y_1+\cdots+y_q}} c(x_1)\cdots c(y_q)\Big]^{1/2q}\\
\le&\frac{1}{|B|}\sum_{z\in B^{-1}A}\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots y_q\\ x_1,\dots,y_q\in Bz}} c(x_1)\cdots c(y_q)\Big]^{1/2q}\\
<&\frac{|B^{-1}A|}{|B|}N^\tau K^\Lambda\Big\{\sum_I\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q\\ (x_1)=\cdots=(y_q)=I}} c(x_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2}\\
\le&\frac{|A^{-1}A|}{|A|}N^{2\tau}K^{2+\Lambda}\Big\{\sum_{I\text{ principal}}\Big[\sum_{\substack{x_1+\cdots+x_q=y_1+\cdots+y_q\\ (x_1)=\cdots=(y_q)=I}} c(x_1)\cdots c(y_q)\Big]^{1/q}\Big\}^{1/2}.
\end{aligned}\tag{9.8}$$

In the first inequality in (9.8), we use that the left side is subconvex as a function of $\{c(x)\}$. The second inequality uses (9.6) which remains valid replacing B by Bz.

This proves (9.2) and Proposition 9.

Proposition 10. *Let $A\subset\mathcal{O}_K$, $|A|=N$ be a finite set of algebraic integers of bounded degree d. Assume*

$$|A.A|<K|A|.\tag{10.1}$$

For $q\in\mathbb{Z}_+,\tau>0$, there is a constant $\Lambda=\Lambda(d,q,\tau)$ such that if $c(x)\in\mathcal{R}_+$ for $x\in A$, we have

$$\begin{aligned}
&\Big[\sum_{\substack{x_1+\cdots+x_q=\\ y_1+\cdots+y_q}} c(x_1)\cdots c(y_q)\Big]^{1/2q}\\
\le&N^\tau K^\Lambda\Big[\sum_{x\in A}c(x)^2\Big]^{1/2}.
\end{aligned}\tag{10.2}$$

Proof.

Decomposing $A=\bigcup_I A_I$ with $A_I=\{x\in A|(x)=I\}$, it suffices by (9.2) to establish (10.2) for each set A_I separately. Since the elements of A_I are conjugate, this amounts to establish (10.2) with A replaced by a set S of units satisfying:

(10.3) The elements of S are of degree at most d.

(10.4) S is contained in a set A satisfying (10.1).

We proceed as follows:

Let S_1 be a maximal subset of S satisfying

$$[\mathbb{Q}(\xi):\mathbb{Q}] = [\mathbb{Q}(\xi,\xi'):\mathbb{Q}(\xi')],$$

if $\xi \neq \xi'$ in S_1.

It follows then from Proposition 5 that the elements of S_1' are multiplicatively independent, where

$$S_1' = S_1 \backslash \{\text{roots of unity}\}.$$

On the other hand, in view of (10.4) and the Plunnecke-Ruzsa inequality

$$\binom{|S_1'|}{\ell} \leq |(S_1')^\ell| \leq |A^\ell| < K^\ell N$$

considering ℓ-fold product sets.

Therefore

$$|S_1'| \lesssim K \log N$$

and also

$$R_1 = |S_1| \lesssim K \log N. \tag{10.5}$$

Decompose next

$$S = \bigcup_{1 \leq \alpha \leq R_1} S^{(\alpha)}, \tag{10.6}$$

where for each α there is an element $\xi_\alpha \in S_1$ with for all $\xi \in S^{(\alpha)}$

$$[K_\alpha(\xi) : K_\alpha] \leq [\mathbb{Q}(\xi):\mathbb{Q}] - 1 \leq d - 1 \tag{10.7}$$

denoting $K_\alpha = \mathbb{Q}(\xi_\alpha)$.

Introducing in (10.2) a factor $K.\log N$, we replace S by $S^{(\alpha)}$ and repeat the process. After d steps at most, we further reduced the problem to the situation where

$S \subset F$, and F is an extension of $\mathbb{Q}$ satisfying $[F:\mathbb{Q}] < C(d)$.

The unit group U of F is of rank $r+s-1 < C(d)$ with r (resp. $2s$) the number of real (resp. complex) places of F. In this situation, the theorem of Evertse, Schlickewei, Schmidt [ESS] applies and implies that for $c(x), x \in U$

$$\Big[\sum_{\substack{x_1+\ldots+x_q= \\ y_1+\cdots+y_q}} c(x_1)\cdots c(y_q) \Big]^{1/2q}$$

$$\leq C(d,q) \Big[\sum c(x)^2 \Big]^{1/2}. \tag{10.8}$$

This completes the proof of Proposition 10.

Obviously the following holds.

Proposition 10′. *Proposition 10 holds for A a set of algebraic numbers (instead of algebraic integers) of bounded degree,*

Theorem 11. *Let A be a finite set of algebraic numbers of bounded degree $\leq d$ and $|A| = N$. Assume*

$$|A.A| < K|A|.$$

Then given any subset $B \subset A$ and finite set $D \subset \mathbb{C}$, we have for arbitrary $\varepsilon > 0$ that

$$|\{(x_1, x_2, y_1, y_2) \in B^2 \times D^2 : x_1 + x_2 = y_1 + y_2\}| < K^{C(d,\varepsilon)} N^{\varepsilon} |B|\,|D|^{1+\varepsilon}. \quad (11.1)$$

In particular

$$|B + D| > K^{-C(d,\varepsilon)} N^{-\varepsilon} |B|\,|D|^{1-\varepsilon}. \quad (11.2)$$

Proof of Theorem 11.

Rewrite (11.1) as

$$\sum_{t \in D} |\{(x_1, x_2, y) \in B^2 \times D : x_1 + x_2 - y = t\}|$$

and using Cauchy-Schwarz, it is bounded by

$$|D|^{1/2} |\{(x_1, x_2, x_3, x_4, y_1, y_2) \in B^4 \times D^2 : x_1 + x_2 - y_1 = x_3 + x_4 - y_2\}|^{1/2}. \quad (11.3)$$

The second factor in expression (11.3) equals

$$\sum_{t \in D} |\{(x_1, x_1, x_3, x_4, y) \in B^4 \times D : x_1 + x_2 - x_3 - x_4 - y = t\}|$$
$$\leq |D|^{1/2} |\{(x_1, \ldots, x_8, y_1, y_2) \in B^8 \times D^2 : x_1 + x_2 - x_3 - x_4 - y_1 = x_5 \cdots - x_8 - y_2\}|^{1/2}$$

Iteration shows that for any specified $s \in \mathbb{Z}_+$ the left side of (11.1) is at most

$$|D|^{1/2+1/4+\cdots+2^{-s}}$$
$$\left|\{(x_1, \ldots, x_{2^{s+1}}, y_1, y_2) \in B^{2^{s+1}} \times D^2 : x_1 + \ldots + x_{2^s} - x_{2^s+1} - \cdots - x_{2^{s+1}} = y_1 - y_2\}\right|^{2^{-s}}$$
$$\leq |D|^{1-2^{-s}} |D|^{2^{-s+1}} |\{(x_1, \ldots, x_{2^{s+1}}) \in B^{2^{s+1}} : x_1 + \cdots + x_{2^s} = x_{2^s+1} + \cdots + x_{2^{s+1}}\}|^{2^{-s}}. \quad (11.4)$$

Apply Proposition 10 (and 8′) with $q = 2^s$ and letting

$$c(x) = \begin{cases} 1 \text{ if } x \in B \\ 0 \text{ otherwise.} \end{cases}$$

We obtain (10.2)

$$|\{(x_1,\dots,x_{2^{s+1}}) \in B^{2^{s+1}} : x_1+\cdots+x_{2^s} = x_{2^s+1}+\cdots+x_{2^{s+1}}\}|^{2^{-s}} \le N^{2\tau}K^{2\Lambda}|B|, \tag{11.5}$$

where $\Lambda = \Lambda(d,s,\tau)$.

Substitution of (11.5) in (11.4) gives as bound in (11.1)

$$N^{2\tau}K^{2\Lambda}|B|\,|D|^{1+2^{-s}}. \tag{11.6}$$

Take $\varepsilon = 2\tau = 2^{-s}$.

Inequality (11.2) follows from (11.1) and

$$|B+D| > \frac{|B|^2|D|^2}{(11.1)}.$$

This proves Theorem 11.

The following result generalizes [BC] to algebraic numbers of bounded degree.

Corollary 12. *For given $d \in \mathbb{Z}_+, m \in \mathbb{Z}_+$, there is $\ell \in \mathbb{Z}_+$ such that the following holds. Let $A, |A| = N$ be a set of algebraic numbers of degree at most d. Then either*

$$|A^\ell| = |\underbrace{A\cdots A}_{\ell\text{-fold}}| > N^m \tag{12.1}$$

or

$$|\ell A| = |\underbrace{A+\cdots+A}_{\ell-\text{fold}}| > N^m. \tag{12.2}$$

Proof.

We first reduce the problem to the case where A is contained in an extension K of $\mathbb{Q}$, $[K:\mathbb{Q}] < C(d)$. Assume (12.1) fails.

We proceed as in earlier arguments.

Let $B_1 \subset A$ be a maximal set such that

$$[\mathbb{Q}(\xi):\mathbb{Q}] = [\mathbb{Q}(\xi,\xi'):\mathbb{Q}(\xi')]$$

for all $\xi \neq \xi'$ in B.

Since the elements of B are multiplicatively independent (after removal of the roots of unity), it follows that

$$N^m \geq |A^\ell| \geq |B^\ell| > \binom{|B|}{\ell} > \Big(\frac{|B|}{2\ell}\Big)^\ell.$$

Hence

$$|B| \lesssim \ell N^{m/\ell}.$$

Therefore there is $\xi_1 \in B$ and $A_1 \subset A$ satisfying

$$|A_1| \gtrsim \frac{1}{\ell} N^{-m/\ell} |A|$$

and denoting $F_1 = \mathbb{Q}(\xi_1)$, for all $\xi \in A_1$

$$[F_1(\xi) : F_1] \leq [\mathbb{Q}(\xi) : \mathbb{Q}] \leq d - 1.$$

Repeat the process with A replaced by A_1.

After d steps, we obtain a subset $A' \subset A$ and en extension field F of $\mathbb{Q}$, $[F : \mathbb{Q}] < C(d) < d^d$ such that $A' \subset F$ and

$$|A'| \gtrsim \frac{1}{\ell^d} N^{1 - \frac{dm}{\ell}} > N^{\frac{1}{2}} \tag{12.3}$$

provided ℓ is taken large enough.

Replace A by A'.

Next, assume ℓ of the form $\ell = 2^t$ with $t \in \mathbb{Z}_+$ large enough. Write

$$N^{2^m} > |A^\ell| = \frac{|A^{2^t}|}{|A^{2^{t-1}}|} \cdot \frac{|A^{2^{t-1}}|}{|A^{2^{t-2}}|} \cdots \frac{|A^2|}{|A|}.$$

Clearly there is some $1 \leq s < t$ and $A_1 = A^{2^s} \subset F$ satisfying

$$|A_1.A_1| < N^{\frac{2m}{t}}.|A_1|.$$

Take $K = N^{\frac{2m}{t}}$ and apply Theorem 11 to the set A_1,

$$|A_1| \leq |A^\ell| < N^{2m}.$$

Take some $x \in A^{2^s - 1}$ and let $B = xA \subset A_1$.

It follows from (11.2) that for any finite $D \subset \mathbb{C}$ and given $\varepsilon > 0$

$$|A + D| > N^{-\frac{2m}{t} C(d,\varepsilon)} N^{-m\varepsilon} |A| \ |D|^{1-\varepsilon}. \tag{12.4}$$

Iterating

$$\begin{aligned} |A + A + D| &> N^{-\frac{2m}{t} C(d,\varepsilon)} N^{-m\varepsilon} |A| \ |A + D|^{1-\varepsilon} \\ &> N^{-\frac{4m}{t} C(d,\varepsilon)} N^{-2m\varepsilon} |A|^{2-\varepsilon} |D|^{1-2\varepsilon} \end{aligned}$$

and after L steps

$$|LA| > N^{-2L\frac{m}{t} C(d,\varepsilon)} N^{-Lm\varepsilon} |A|^{L - L\frac{(L-1)}{2}\varepsilon}. \tag{12.5}$$

It remains to specify the parameters.

Take $L = m + 1, \varepsilon = \frac{1}{10L^2}, t = {}^2 \log \ell > 10C(d,\varepsilon)m^2$.

It follows that

$$|\ell A| > |LA| > |A|^m.$$

This proves Corollary 12.

§3. Product sets of algebraic numbers of bounded degree and small height.

We will show the following.

Proposition 13. *Let A be a finite set of algebraic integers of degree at most d and such that for all $x \in A$*

$(*)$ *the minimal polynomial of x over $\mathbb{Q}$ has coefficients bounded by M.*

Then for $(c_x)_{x \in A}$ in $\mathbb{R}_+$ and any fixed $q \in \mathbb{Z}_+$, we have

$$\begin{aligned} &\Big[\sum_{\substack{x_1 \cdots x_q = \\ y_1 \cdots y_q}} c_{x_1} \cdots c_{x_q} c_{y_1} \cdots c_{y_q} \Big]^{1/2q} \\ \leq \ &\Big(\exp C(d,q) \frac{\log M}{\log \log M} \Big) \sqrt{\sum c_x^2} \ . \end{aligned} \tag{13.1}$$

Corollary 14. *Let A be as in Proposition 13. Then or any given ℓ*

$$|\underbrace{A\cdots A}_{\ell\text{-fold}}| \geq \frac{1}{\exp C(d,\ell)\frac{\log M}{\log\log M}}|A|^{\ell}. \tag{13.2}$$

Application with $\ell = 2$ yields Proposition 14' stated in the introduction.

Proof of Proposition 13.

In order to setup an inductive argument, we make the following assumptions:

Let K be an extension of $\mathbb{Q}, [K:\mathbb{Q}] = d_1$ and let A be as above such that

$$[K(x):K] \leq d_2 \text{ for all } x \in A. \tag{13.3}$$

We establish (13.1) by induction on d_2.

If $d_1 = 1$, then $A \subset K$. Use the division theory in $\mathcal{O}_K$. Thus factoring principal ideals in prime ideals, we have for $t \in \mathcal{O}_K$, t not a unit

$$\begin{aligned} &|\{I : I \text{ ideal in } \mathcal{O}_K \text{ dividing } (t)\}| \\ <&\exp C(d_1)\frac{\log N_{K/\mathbb{Q}}(t)}{\log\log N_{K/\mathbb{Q}}(t)}. \end{aligned} \tag{13.4}$$

Hence, for given $t \in \mathcal{O}_K$ obtained as a product of q elements from A, we obtain

$$\begin{aligned} &|\{(x_1,\dots,x_q) \in A : x_1\cdots x_q = t\}| \\ \leq&|\{I : I \subset \mathcal{O}_K \text{ ideal dividing } (t)\}|^q\big(\max_{x\in A}|\{x' \in A : (x) = (x')\}|\ \big)^q \\ \lesssim&(\exp C(d_1)q\log M^q/\log\log M)(\log M)^{d_1 q}. \end{aligned} \tag{13.5}$$

We used here (13.4) and an estimate on the number of units in $\mathcal{O}_K$ which minimal polynomial has coefficients bounded by $M^{C(d_1)}$.

Hence

$$\begin{aligned} &\sum_{\substack{x_1\cdots x_q = \\ y_1\cdots y_q}} c_{x_1}\cdots c_{x_q}c_{y_1}\cdots c_{y_q} \\ =&\sum_t\Big(\sum_{x_1\cdots x_q = t} c_{x_1}\cdots c_{x_q}\Big)^2 \\ \leq&(13.5)\ \Big(\sum c_x^2\Big)^q \end{aligned} \tag{13.6}$$

and (13.1).

Next we show how to perform the inductive step.

Let

$$A' = A \cap (K.\{\text{roots of unity}\}).$$

Since the roots of unity that may occur from A form a set of size at most $C(d)$, (13.1) holds for the subset A' (as a consequence of the $d_2 = 1$ case).

We may therefore assume that $A \cap K.\{\text{roots of unity}\}=\phi$.

Assume

$$[K(\xi) : K] = d_2 \text{ for all } \xi \in A. \tag{13.7}$$

Take $q = 2$ for simplicity (the general case is similar).

We will apply Proposition 5.

Let x_1, x_2, y_1, y_2 be distinct elements in A and suppose we have a relation $x_1x_2 = y_1y_2$. Hence $S = \{x_1, x_2, y_1, y_2\}$ do not form a multiplicatively independent set and by Proposition 5, there are $\xi \neq \xi'$ in S such that

$$[K(\xi) : K] > [K(\xi', \xi) : K(\xi')]. \tag{13.8}$$

From (13.8), there is a nontrivial polynomial $X^r + \sum_{s=0}^{r-1} P_s(\xi')X^s \in K(\xi')[X]$ of degree $r \leq d_2 - 1$ such that

$$\xi^r + \sum_{0 \leq s < r} P_s(\xi')\xi^s = 0. \tag{13.9}$$

Let $\xi_1, \ldots, \xi_{d_2}$ be the conjugates of ξ over K and denote $F_\xi = K(\xi_1, \ldots, \xi_{d_2})$ the splitting field of ξ over K. Similar for ξ'.

Since $X^r + \sum_{s=0}^{r-1} P_s(\xi')X^s$ divides the minimal polynomial of ξ over K, its (distinct) roots are contained in $\{\xi_1, \ldots, \xi_{d_2}\}$. This clearly implies that

$$\{P_s(\xi') : 0 \leq s \leq r-1\} \subset F_\xi$$

and therefore, by (13.9)

$$[(F_\xi \cap F_{\xi'})(\xi) : F_\xi \cap F_{\xi'}] \leq r \leq d_2 - 1. \tag{13.10}$$

Since (13.8) is symmetric in ξ, ξ', also

$$[(F_\xi \cap F_{\xi'})(\xi') : F_\xi \cap F_{\xi'}] \leq d_2 - 1. \tag{13.11}$$

We introduce the following definition.

Given an extension field L of K with $[L:K] \le d_2!$ denote

$$A_L = \{x \in A : K \subset L \subset F_x \text{ and } [L(x):L] \le d_2 - 1\}. \tag{13.12}$$

The preceding shows that if $x_1, x_2, y_1, y_2 \in A$ satisfy $x_1 x_2 = y_1 y_2$, then there is a pair of elements $\xi \ne \xi'$ in $\{x_1, x_2, y_1, y_2\}$ and an extension L of K such that $\xi, \xi' \in A_L$. Next, write

$$\begin{aligned}(13.13) = &\sum_{x_1 x_2 = y_1 y_2} c_{x_1} c_{x_2} c_{y_1} c_{y_2} \\ = &\sum_L \sum_{\substack{x_1, x_2 \in A_L \\ x_1 x_2 = y_1 y_2}} c_{x_1} c_{x_2} c_{y_1} c_{y_2} \qquad (13.14) \\ &+ \sum_L \sum_{\substack{x_1, y_1 \in A_L \\ x_1 x_2 = y_1 y_2}} c_{x_1} c_{x_2} c_{y_1} c_{y_2} \qquad (13.15) \\ &+ \ \varpi,\end{aligned}$$

where ϖ refers to the other sums corresponding to $x_1, y_2 \in A_L$; $x_2, y_1 \in A_L$; $x_2, y_2 \in A_L$ and $y_1, y_2 \in A_L$.

We estimate (13.15) for instance. By Cauchy-Schwartz

$$\begin{aligned}(13.15) = &\sum_t \Big[\sum_L \sum_{x_1, y_1 \in A_L, \frac{x_1}{y_1} = t} c_{x_1} c_{y_1}\Big]\Big[\sum_{x_2, y_2 \in A_L, \frac{y_2}{x_2} = t} c_{x_2} c_{y_2}\Big] \\ &\le \Big(\sum_t \Big[\sum_L \sum_{x_1, y_1 \in A_L, \frac{x_1}{y_1} = t} c_{x_1} c_{y_1}\Big]^2\Big)^{1/2} \Big(\sum_t \Big[\sum_{x_2, y_2 \in A_L, \frac{y_2}{x_2} = t} c_{x_2} c_{y_2}\Big]^2\Big)^{1/2} \\ &= (13.16).(13.17),\end{aligned}$$

where

$$(13.17) = \sqrt{(13.13)}$$

and

$$(13.16) \le \sum_L \Big\{\sum_t \Big[\sum_{\substack{x_1, y_1 \in A_L \\ \frac{x_1}{y_1} = t}} c_{x_1} c_{y_1}\Big]^2\Big\}^{1/2}. \tag{13.18}$$

For fixed L, it follows from the induction hypothesis that

$$\begin{aligned}\sum_t \Big[\sum_{\substack{x_1, y_1 \in A_L \\ x_1/y_1 = t}} c_{x_1} c_{y_1}\Big]^2 &= \sum_{\substack{x_1, x_2, y_1, y_2 \in A_L \\ x_1 x_2 = y_1 y_2}} c_{x_1} c_{x_2} c_{y_1} y_{y_2} \\ &< \Big(\exp C(d)) \frac{\log M}{\log\log M}\Big)\Big(\sum_{x \in A_L} c_x^2\Big)^2. \qquad (13.19)\end{aligned}$$

Substituting (13.19) in (13.18) and collecting estimates we get

$$\sqrt{(13.13)} \lesssim \big(\exp C(d)\frac{\log M}{\log\log M}\big)\Big(\sum_L \sum_{x\in A_L} c_x^2\Big). \tag{13.20}$$

To conclude the argument, it remains to observe that

$$\begin{aligned}|\{L : x \in A_L\}| \leq & |\{L : K \subset L \subset F_x\}| \\ = & |\{\text{subgroups of } \mathrm{Aut}_K F_x\}| \\ \leq & |\{\text{subgroups of } \mathrm{Sym}(d)\}| < C(d).\end{aligned}$$

This proves Proposition 13.

§4. An application to incidence geometry.

Using Proposition 8 (instead of [BC]) and the argument from [CS], we obtain the following geometric statement, generalizing Theorem 6.1 in [CS].

We denote by $\mathcal{P}_d$ the set of points in $\mathbb{C}\times\mathbb{C}$ with algebraic coordinates of degree at most d.

Theorem 15. *Given $d \in \mathbb{Z}_+$ and $\epsilon > 0$, there is $\delta > 0$ such that for any P_1, P_2, P_3 noncollinear, and $Q_1, \cdots, Q_n \in \mathcal{P}_d$, if*

$$|\{L(P_i, Q_j) : 1 \leq i \leq 3, 1 \leq j \leq n\}| \leq n^{1/2+\epsilon}, \tag{15.1}$$

then for any $P \in \mathbb{C}\times\mathbb{C} \setminus \{P_1, P_2, P_3\}$, we have

$$|\{L(P, Q_j) : 1 \leq j \leq n\}| > n^{1-\delta}. \tag{15.2}$$

The proof is identical to that of Theorem 6.1 in [CS] and we will not repeat it here. The only difference is that $\mathbb{Q}\times\mathbb{Q}$ is replaced by $\mathcal{P}_d$ and we use Proposition 8 instead of [BC].

References

[BC]. J. Bourgain, M.-C. Chang, *On the size of k-fold sum and product sets of integers*, JAMS 17(2) (2004), 473-497.

[C1]. M.-C. Chang, *A sum-product estimate in algebraic division algebra over R*, Israel J. Math, 150 (2005), 369-380.

[C2]. _____, *Factorization in generalized arithmetic progressions and applications to the Erdos-Szemeredi sum-product problems*, Geom. Funct. Anal. Vol. 13 (2003), 720-736.

[C3]. _____, *Sum and product of different sets*, Contributions to Discrete Math. Vol 1, 1 (2006), 57-67.

[CS]. M.-C. Chang, J. Solymosi, *Sum-product theorems and incidence geometry*, J. Eur. Math. Soc. 9 , no. 3, (2007), 545–560.

[El]. G. Elekes, *On the number of sums and products*, Acta Arithmetica 81, Fase 4, 365-367 (1997).

[ES]. P. Erdős, E. Szemerédi, *On sums and products of integers*, in 'Studies in Pure Mathematics', Birkhauser, Basel, (1983), 213-218.

[ESS]. J.-H. Evertse, H. Schlickewei, W. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math 155, (2002), 807-836.

[NT]. M. Nathanson, G. Tenenbaum, *Inverse theorems and the number of sums and products*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[So]. J. Solymosi, *Bounding multiplicative energy by the sumset*, (preprint).

[St]. H.M. Stark,, *A transcendence theorem for class-number problems*, Ann. of Math. 94, no. 1, (1971), 153-173.

[TV]. T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

[T]. G. Tenenbaum, *Sur la répartition des diviseurs*, Séminaire Delange-Pisot-Poitou. Théorie des nombres, 17 no. 2 (1975-1976)Exp. No. G14, 5 p.