Team France 3

5. **Stable Polygons**

Abstract

In this problem, we study the subsets of a regular polygon having for center of gravity the center of the polygon. To this, we identify the vertices of the polygon with the roots of unity, which lead us to have some analytic considerations. We also used arithmetic and combinatorics properties in order to count such subsets.

We solved completly the first question, using the irreducibility of cyclotomic polynomials on $\mathbb{Q}$ in order to show that a stable subset was the entire polygon or the empty set ; Then, we solved partly the following questions, introducing the notion of "elementary subset", in order to decompose any stable subset of the polygon in such subsets.

Some preliminary results

Reformulation of the problem

Let $P_n = \{A_0, \ldots, A_{n-1}\}$ be the set of vertices of a regular polygon with n sides. In the complex plane, we can set the regular polygon such that for any $k \in \{0, \ldots, n-1\}$ the affix of A_k is $e^{\frac{2i\pi k}{n}}$. Let $\zeta_n = e^{\frac{2i\pi}{n}}$. Then a subset $\{A_{k_1}, \ldots A_{k_t}\}$ of P_n is stable if and only if $\zeta_n^{k_1} + \ldots \zeta_n^{k_t} = 0$. From now on we are going to identify a point with its affixe.

Elementary properties

It is easy to see that stable sets have three following properties :

1. the reunion of stable disjoined subsets is a stable subset too (one can remark it by writing the vectorial equality defining the gravity center). We call this property the "disjoined reunion property".
2. If a is a strict divisor of n, there exist a regular $\frac{n}{a}$-gons with vertices of the n-gon, which are all stable subsets. These subsets make a partition of the vertices of the n-gon. We call this the "rotation stability property".
3. If E is a stable set andE' is a stable subset, then $E \setminus E'$ is also stable. We call this the "difference property".

Remark 1 *By the difference property, the empty set is stable.*

Roots of unity.

Definition 1 *Be $n \in \mathbb{N}^*$. $\zeta \in \mathbb{C}$ is said to be an n-th root of unity if $\zeta_n = 1$. And if $\forall m \in \{1, \ldots, n-1\}$ $\zeta^m \neq 1$, ζ is said to be a primitive root.*

Theorem 1 *$\zeta \in \mathbb{C}$ is an n-th root of unity if and only if there is an integer k such as $0 \leq k \leq n-1$ and*

$$\zeta = e^{\frac{2i\pi k}{n}}.$$

ζ is a primitive root of unity if and only if k and n are coprime .

Proof : The n-th roots of unity are the roots of the polynomial $X^n - 1$. There are at most n roots, and one verifies easily that the n ζ described above are different and roots of the polynomial, so that we can identify them with these roots.
And, for all integer k such as $0 \leq k \leq n-1$, the smallest integer m such as $\zeta^m = 1$ is $m = \frac{n}{gcd(k,m)}$. The conclusion follows.
We obtain easily the following results :

Corollary 1 *1. There are exactly $\varphi(n)$ primitive roots of unity, where φ is Euler's totient function.*

2. If n is prime, then all n-th roots of 1 are primitive.

3. If n is not prime, then an n-th root of 1 is a d-th primitive root of 1 for a certain $d|n$.

4. If ζ_n is a primitive n-th root of unity then any n-th root of the unity is a power of ζ_n (in other words $\{\zeta \mid \zeta^n = 1\} = \{\zeta_n^a \mid a \in \{0, \dots, n-1\}\}$).

Then finding all the stable subsets in P_n is similar as finding all the sets $\{k_1, \dots, k_t\}$ such that $t \leq n$, $\forall j \in \{1, \dots, t\}$ $0 \leq k_j < n$ and $\zeta_n^{k_1} + \cdots + \zeta_n^{k_t} = 0$.

Here are two well-known results about sums of roots of unity.

Theorem 2 *Let n a positive integer, the sum of all n-th roots of unity is zero. ie, if ζ_n is a primitive n-th root of unity, then*

$$1 + \zeta_n + \cdots + \zeta_n^{n-1} = 0.$$

In fact, this is a geometric sum and the set of the n first powers of a primitive n-th root of the unity is the set of all n-th root of the unity (since we have $\zeta_n = e^{\frac{2ik\pi}{n}}$ where k is an additive generator modulo n).

Theorem 3 *Let p be a prime number and ζ_p a primitive p-th root of unity. Let $k \in \mathbb{N}$ be such that $1 < k \leq p-2$. Then for all $n_1, \dots, n_k \in \{0, \dots, p-2\}$ pairwise distinct :*

$$S = \sum_{i=1}^{k} \alpha_i \zeta_p^{n_i} = 0,\ \alpha_i \in \mathbb{Q}\ \forall i \Longleftrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0.$$

Proof : S is a polynomial in ζ_p. Suppose that there exist a such polynomial that is not the zero polynomial. Consider a such polynomial T of minimal degree, with $T(\zeta_p) = 0$. Suppose $degT > 0$.

Let P the cyclotomic polynomial of order n on $\mathbb{Q}$:
$P(X) = \frac{X^n - 1}{X - 1} = \sum_{i=0}^{n-1} X^i$
Remark that ζ_p is a root of it (by theorem 1). We first prove its irreducibility on $\mathbb{Q}$.

To this we use Eisenstein's criterion with a new variable that we find after a translation : $X = Y + 1$

The new polynomial can now be written : $P(Y+1) = \frac{(Y+1)^n - 1}{Y}$

The highest degree of coefficient will be equal to 1 because $\binom{n-1}{0} = 1$, so one of the conditions of the criterion is respected.

Call a_i the coefficient of X^i for all i. We have $a_0 = n$ thus $n \mid a_0$ but n^2 doesn't divide a_0 so another condition is respected. And for all i such that $1 \leq i \leq n-2$, we have by the binom's formula :

$a_i = \binom{n}{i+1}$. And, $n! = a_i \times (i+1)! \times (n-i-1)!$. Since n is prime, and using Euclid's lemma, we have :

$$n \mid a_i$$

Thus, Eisenstein's criterion is fully respected, so that P is irreducible on $\mathbb{Q}$

In $\mathbb{Q}[X]$, we can use the Euclidian division, so that :

$$P(X) = K(X)T(X) + R(X)$$

, where K and R are polynoms with rationnal coefficients, and $degR < degT$. Moreover, the irreducibility of P is enough to say that R isn't the zero polynomial. This contradicts the fact that the degree of T is minimal. Thus, there isn't any polynomial of degree smaller or equal to $n-2$ that has ζ_p as a root. Thus,

$$\alpha_1 = ... = \alpha_k = 0.$$

The reciprocity is easy to verify.

When n is a prime number.

Let $n = p$ be an odd prime number.

Cosider $A \subseteq P_p$.

- If $\#A = p$ then
$$\sum_{i=0}^{p-1} \zeta_p^i = 0$$
according to the theorem 2.
- If $\#A < p$ then there is $\alpha_1, \ldots, \alpha_p \in \{0; 1\}$, not all equal to 0 such that
$$\sum_{i=0}^{p-2} \alpha_i \zeta_p^i = 0,$$
that contradicts the theorem 3. So there is no stable subset A with $\#A < p$.

Then the only stable subsets of P_p are P_p and the empty set.

Case $n = pq$.

Let $n = pq$, where p, q are two dinstict prime numbers.

Definition 2 *Let's call* ***elementary stable sets*** *the sets*

$$E_{a,l} = \{\zeta_{pq}^a, \zeta_{pq}^a \zeta_l, \dots, \zeta_{pq}^a \zeta_l^{l-1}\},$$

where $l \in \{p, q\}$.

In other words, an elementary stable set is a subset of the polygon and is a regular polygon itself with a prime number of sides, that is p or q here. This definition can be extended to any n (not only $n = pq$). In every case, the cardinality of a such subset divides n. Obviously, any elementary stable set $E_{a,l}$ is stable :

$$\zeta_{pq}^a + \zeta_{pq}^a \zeta_l + \cdots + \zeta_{pq}^a \zeta_l^{l-1} = \zeta_{pq}^a (1 + \zeta_l + \cdots + \zeta_l^{l-1}) = 0.$$

So any disjoint reunion of elementary stable sets is stable.

Lemma 1 *The elementary stable sets have the two following properties.*

1. *The sets* $E_{0,p}, \dots E_{q-1,p}$ *are distinct and* $\forall a, b \in \{0, \dots, q-1\}$ *such that* $a \neq b$, $E_{a,p} \cap E_{b,p} = \emptyset$ *et* $\bigcup_{a=0}^{q-1} E_{a,p} = \{1, \zeta_n, \dots \zeta_n^{n-1}\}$.
2. *The sets* $E_{0,q}, \dots E_{p-1,q}$ *are distinct and* $\forall a, b \in \{0, \dots, p-1\}$ *such that* $a \neq b$, $E_{a,q} \cap E_{b,q} = \emptyset$ *and* $\bigcup_{a=0}^{p-1} E_{a,q} = \{1, \zeta_n, \dots \zeta_n^{n-1}\}$.

This is a corollary of the rotation stability property.

Lemma 2 *Let* $a \in \mathbb{N}$ *be such that* $0 \leq a < p-1$. *Then* $E_{a,p} \cap E_{0,q} \neq \emptyset$.

Proof :

The set $E_{a,p} \cap E_{0,q}$ is non empy if and only if there exists a $b \in \{0; p-1\}$ such that $\zeta_{pq}^a \zeta_p^b \in \{1, ..., \zeta_q^{q-1}\}$.

The numbers p, q are distinct primer numbers, so coprime. So there exist $x, y \in \mathbb{Z}$ such that $xp + yq = a$. So $\forall b \in \{0; p-1\}$

$$\zeta_{pq}^a \zeta_p^b = e^{\frac{a2i\pi}{pq}} e^{\frac{b2i\pi}{p}} = e^{\frac{2i\pi(xp+yq)}{pq}} e^{\frac{2i\pi b}{p}} = e^{\frac{2i\pi x}{q}} e^{\frac{2i\pi(y+b)}{p}}.$$

There exist $y_1 \in \mathbb{Z}$ and $r_1 \in \{0; p-1\}$ such that $y = y_1 p + r_1$. So if we take $b = p - r_1$ we get $0 \leqslant b < p$ and

$$\zeta_{pq}^a \zeta_p^b = e^{\frac{2i\pi x}{q}} e^{\frac{2i\pi(y_1 p + r_1 + p - r_1)}{p}} = e^{\frac{2i\pi x}{q}} e^{\frac{2i\pi p(y_1+1)}{p}} = e^{\frac{2i\pi x}{q}} \in E_{0,q}.$$

So $E_{a,p} \cap E_{0,q} \neq \emptyset$. $\square$

There is no disjoint reunion of elementary stable sets of different cardinality (because every $E_{b,q}$ is obtained from $E_{0,q}$ by multiplying all the terms by some ζ_{pq}^{a}). So the only reunion of elementary sets that are stable are of cardinality $p, 2p, 3p, ..., pq$ (reunion of $E_{a,p}$) or $q, 2q, 3q, ..., pq$ (reunion of $E_{b,q}$). As p and q are different prime numbers, $ap \neq bq$ if $0 < a < q$ and $0 < b < p$.

Now we only need to find in how many different ways we can choose the elementary stable sets to obtain a stable polygon in P_n. Using the disjoined reunion and the rotation stability properties, we obtain that any reunion of regular p-gons (having vertices of the n-gon) or of regular q-gons is a stable subset. In addition, there are q such p-gons, and p such q-gons.

Thus, there are 2^p stable subsets that are reunion of q-gons, and 2^q stable subsets that are reunion of p-gons. Here, we counted twice the empty set and twice the entire n-gon, so that we obtain $2^p + 2^q - 2$ stable subsets. Here we conjecture that any stable subset is the reunion of disjoined elementary subsets. Thus, any else stable subset contains the reunion of a regular p-gon and of a regular q-gon.

Conjecture : Any stable set is either an elementary stable or the disjoint reunion of stable elemenatary sets.

In the case $n = 2p$, the conjecture holds : there are only two different elementary stable sets E_p and E'_p such that $\#E_p = \#E'_p = p$.

We know that :

1. $E_p \cap E'_p = \emptyset$ by the rotation stability property.
2. if $\zeta_{2p}^{\alpha} \in E'_p$ then $-\zeta_{2p}^{\alpha} \notin E'_p$

Consider a stable set X

* Case $\#X > p$
  There is $\alpha \in \{0, 2p-1\}$ such that $\zeta_{2p}^{\alpha}, -\zeta_{2p}^{\alpha} \in X$ And $\{\zeta_{2p}^{\alpha}, -\zeta_{2p}^{\alpha}\}$ is stable by the difference property. Then $X_1 = X \setminus \{\zeta_{2p}^{\alpha}; -\zeta_{2p}^{\alpha}\}$ is also stable with a cardinality equal to $\#X - 2$. We can repeat this operation as long as possible and we can finally suppose that $\#X \leqslant p$ and for any α such that $\zeta_{2p}^{\alpha} \in X$ and $-\zeta_{2p}^{\alpha} \notin X$.
* Case $\#X = p$ Then we have two cases :
  (a) X is equal to E_p or X is equal to $E'p$

(b) If X is different from E_p and from E'_p
Then there is α such that : $\zeta_{2p}^{\alpha} \in E_p \cap X$
And there is β such that : $\zeta_{2p}^{\beta} \in E_p \cap X$

We know that X is stable, so :

$$\sum \zeta_{2p}^{\alpha i} + \sum \zeta_{2p}^{\beta j} = 0$$

and every $\zeta_{2p}^{\alpha i} \in E_p$ and every $\zeta_{2p}^{\beta j} \in E'_p$.
Then $-\sum \zeta_{2p}^{\alpha i} + \sum \zeta_{2p}^{\beta j} = 0$ (1)
but $-\zeta_{2p}^{\alpha i} \in E'_p$ and $\forall i, j \zeta_{2p}^{\alpha i} \neq \zeta_{2p}^{\beta j}$

Suppose $E_p = E'_p$ then

$$\sum_{a=0}^{p-1} \zeta_{2p}^{2a} = 0(2)$$

and

$$(1) + (2) \Longrightarrow 2 \sum \zeta_{2p}^{\beta j} = 0$$

Thus, this supposition leads to a contradiction.

Therefore, there are couples such that $\zeta_n^{\alpha} = -\zeta_n^{\beta}$ or $-\zeta_n^{\beta} = \zeta_n^{\alpha} * \zeta_2$ so ζ_n^{β} and ζ_n^{α} make a elementary stable set with two elements and with $\zeta_n^{\beta} \in E'_p$ and $\zeta_n^{\alpha} \in E_p$

Case $n = p^k$.

Suppose $n = p^k$ where p is a prime number and $k \in \mathbb{N}$.
We want to establish the following formula :

$$N = 2^{p^{q-1}}.$$

Again, we suppose that any stable subset is the reunion of disjoined non-empty elementary subsets. Consider c the cardinality of an elementary subset, since its vertices are regularly placed on the n-gon, we have $c \mid n$. Since c is prime, $c = p$. Therefore, there are p^{q-1} elementary subsets, that is the p^{q-1} different p-gons with vertices of the n-gon.
Using the same counting argument as in the second question, we obtain the result.

Case of n arbitary number.

We divide n into product of prime numbers and we get $n = p_1^k 1 * p_2^k 2 * p_3^k 3 * ... * p_m^k m$ We treat this question as the last one, but we consider m elementary stable sets, so the only reunions of elementary stable sets are of cardinality $p_1, 2p_1, 3p_1, ..., (n/p_1)$ and $p_2, 2p_2, 3p_2, ..., (n/p_2)$ and ... and $p_m, 2p_m, 3p_m, ..., (n/p_m)$. It remains to know in how many different ways we can choose the elementary stable sets so as to obtain a stable polygon in P_n If we reuse the result of the last question, we find that the sum of the reunion of the elementary stable sets is equal to :

$$\sum_{i=1}^{p_i=m} \sum_{j=1}^{n/p_i} \binom{n/p_i}{j} - (m-1)$$

We have to substract $m - 1$ because we count m times the polygon itself. This formula stays an estimation, without proof for it.

1 Further ideas.

We can imagine an analogous problem in 3 dimensions, with polyhedrons.