PROBLEM 3

FRANCE 2

We completly solved questions 1) a) and b), 2) a). We partially solved 3) a) and b).

In 1) a), we used algebraic number theory (in particular the arithmetic of ideals) to prove that the z_i are algebraic integers.

In 2) a), we used analytic methods, which can't be generalized to the complexe case which should use algebraic number theory and therefore "only" algebraic methods.

In 3) a) we find an interesting necessary condition and we solved in particular the case the real case. The complex case seems to be related to how well can irational numbers be approximated by rational numbers.

In 3) b) we also find a quite restrictive necessary condition and we solved the real case. The complex case seems to be related to cyclotomic polynomials and we only solved completely a particular case for p-th roots of unity.

Question 1 (a). We recall the Newton–Girard formulae :
Let n an integer ≥ 2, $(z_1, ..., z_n) \in \mathbb{C}^n$. We consider $S_k = \sum_{i=1}^n z_i^k$. We note $\sigma_1, ..., \sigma_n$ the the elementary symmetrics functions of z_i.

$$\sigma_k = \sum_{1\leq i_1<...<i_k\leq n} z_{i_1}...z_{i_n}$$

We have for all p $\in \{1, ..., n-1\}$

$$S_p = \sigma_1 \cdot S_{p-1} - \sigma_2 \cdot S_{p-2} + ... + (-1)^{p-2} \cdot \sigma_{p-1} \cdot S_1 + (-1)^{p-1} \cdot p \cdot \sigma_p$$

Démonstration. Let $p \in \{1, ..., n-1\}$.Let's compare S_p and $\sigma_1 S_{p-1}$, we obtain :

$$S_p = \sigma_1 S_{p_1} - \sum_{i_1\neq i_2} z_{i_1} z_{i_2}^{p-1}$$

Then let's do the same thing with this last sum and $\sigma_2 S_{p-2}$. We have :

$$\sigma_2 S_{p-2} = S_p = \sum_{i_1\neq i_2} z_{i_1} z_{i_2}^{p-1} + \sum_{\substack{1\leq i_1<i_2\leq n \\ i_3\neq i_1,i_2}} z_{i_1} z_{i_2} z_{i_3}^{p-2}$$

Note

$$A_k = \sum_{\substack{1\leq i_1<...<i_k\leq n \\ i_{k+1}\neq i_1,i_2,...,i_k}} z_{i_1}...z_{i_k} z_{i_{k+1}}^{p-k}$$

We notice in particular that $A_0 = S_p$ and $A_{p_1} = p\sigma_p$.We obtain for $1 \leq k \leq p-1$

$$\sigma_k S_{p_k} = A_{k-1} + A_k$$

Multiplying the first relation by -1, the second by $(-1)^2$, ..., and the $(p-1)$th by $(-1)^{p-1}$, we found :

$$\sum_{k=1}^{p-1} (-1)^k \sigma_k S_{p-k} = \sum_{k=1}^{n} (-1)^k (A_{k-1} + A_k) = -A_0 + (-1)^{p-1} A_{p-1} = -S_p + (-1)^{p-1} p\sigma_p$$

And the result follows. □

Using these formulae, an immediate induction shows that for all $1 \leq i \leq n$, $\sigma_i \in \mathbb{Q}$ and if $\sigma_i = \frac{p_i}{q_i}$ with $\gcd(p_i, q_i) = 1$, then q_i divided $n!$.
We can write $z_i^n - \sigma_1 z_i^{n-1} + ... + (-1)^{n-1}\sigma_{n-1} z_i + (-1)^n \sigma_n = 0$. Multiplying by $n!^n$, we obtain :

$$(n!z_i)^n - n!\sigma_1 (n!z_i)^{n-1} + ... + (-1)^{n-1} n!^{n-1} \sigma_{n-1} (n!z_i) + (-1)^n n!^n \sigma_n = 0$$

and we found that $n!z_i$ is an algebraic integer (it's a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$). More generally, let $z_i^{'} = z_i^k$ for a $k \geq 0$, by hypothesis the newton sums associated to the z_i' are integers. With the same argument as previously, we find that $n!z_i^{'}$ is an algebraic integer. Hence, we have $\forall k \geq 0, \quad n!z_i^k$ algebraic integer.
Let $K = \mathbb{Q}(z_1, ..., z_n) := \{Q(z_1, ..., z_n), Q \in \mathbb{Q}[X_1, ..., X_n]\}$ be the field generated by z_1, ..., z_n. Let $\mathcal{O}_K$ the set of the algebraic integer in K. We can prove that $\mathcal{O}_K$ is a ring (cf appendix).

For the next, we need the following lemma :

Lemma. Let K a number field, $\mathcal{O}_K$ his ring of integers and x an element in K. If $\exists N \in \mathbb{N}^* \mid \forall k \geq 0, \quad Nx^k \in \mathcal{O}_k$, then $x \in \mathcal{O}_k$

Proof. By definition, $A = \mathcal{O}_k$ is a Dedekind's ring, i.e each ideal of A can be written uniquely as a product of prime ideals. Note $y = N \cdot x \in \mathcal{O}_k$. We know that $Nx^k = \dfrac{y^k}{N^{k-1}} \in \mathcal{O}_k$ for all $k \geq 1$. If we write $(y) = \mathfrak{p}_1^{\alpha_1} ... \mathfrak{p}_r^{\alpha_r}$, $(N) = \mathfrak{p}_1^{\beta_1} ... \mathfrak{p}_r^{\beta_r}$ and $(y)^k = \left(Nx^k\right) \cdot (N)^{k-1}$. Then, we see that $\forall 1 \leq i \leq n$ and $k \geq 1$, $k \cdot \alpha_i \geq (k-1) \cdot \beta_i$, so when $k \longrightarrow \infty$, we have $\alpha_i \geq \beta_i$. So $(y) \subset (N)$. So $y = N \cdot z$ with some $z \in \mathcal{O}_k$. Hence $z = x \in \mathcal{O}_K$.

Using the lemma, applied to K defined previously, we find that the z_i are algebraic integers. Then the σ_k are algebraic integers, since the product and the sum of two algebraic numbers is an algebraic number (cf appendix). So σ_k are rationnals and algebraic integers, so they are in $\mathbb{Z}$. Indeed, if $\dfrac{a}{b}$ with $gcd(a, b) = 1$ is an algebraic integer, there exists a monic polynomial $P \in \mathbb{Z}[X]$ such that :

$$\sum_{k=0}^{n} a_k \left(\frac{a}{b}\right)^k = 0$$

Multiplying by b^n, we obtain

$$a^n + \sum_{k=0}^{n-1} a_k a^k b^{n-k} = 0$$

So $b \mid a^n$ and $b = 1$.

Hence $P(X) \in \mathbb{Z}[X]$

Question 1 (b). Let $S_k = \sum_{i=1}^n z_i^k$.

Since z_i are rational numbers, we can write $z_i = \frac{a_i}{b_i}$ and $S_k = \sum_{i=1}^n \left(\dfrac{a_i}{b_i}\right)^k$ for some coprime integers a_i and b_i. Let N the lcm of the b_i. We have $S_k = \sum_{i=1}^n \left(\frac{c_i}{N})^k\right)$ with $c_i = N \cdot z_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.

Factoring by N, we obtain $S_k = \frac{\sum_{i=1}^n c_i^k}{N^k}$. Since S_k is integer for all $k \geq 1$, N^k divides $\sum_{i=1}^n c_i^k$ for all $k \geq 1$. Assume that $N \neq 1$. Let $p \in \mathbb{P}$ (set of the prime integers) such that p divides N. Denote by n' the number of c_i that are coprime with p.

We have

$$\sum_{i=1}^{n} c_i^k = \sum_{c_i \wedge p = 1} c_i^k + \sum_{c_i \wedge p \neq 1} c_i^k$$

Taking $k = \varphi(p^\alpha)$, we obtain for all $\alpha \geq 1$, $\sum_{c_i \wedge p=1} c_i^k + \sum_{c_i \wedge p \neq 1} c_i^k \equiv 0 \bmod p^\alpha$.
We know that $p^\alpha \mid p^{\varphi(p^\alpha)}$ (because $\varphi(p^\alpha) \geq p^{\alpha-1} \geq 2^{\alpha-1} \geq \alpha$ if $\alpha \geq 1$) and $\sum_{c_i \wedge p=1} c_i^k$ and $\sum_{c_i \wedge p \neq 1} c_i^k$ are respectively congruent to n' and 0 modulo p^α, we obtain that p^α divides n' for all $\alpha \geq 1$. So $n' = 0$ and p divides all c_i. Dividing N and the c_i by p, we repeat the operation with $\dfrac{N}{p}$ and $\dfrac{c_i}{p}$ and we notice that $\forall p \in \mathbb{P}, \forall \alpha \geq 1, p^\alpha \mid N \Longrightarrow p^\alpha \mid c_i$ i.e $N \mid c_i$. So z_i are integers.

Remark : in fact this question is an immediate consequence of question 1) a) which shows that the z_i are algebraic integers, because we know that an algebraic integer which is a rational number is an integer (cf annexe).

Question 2 (a). We suppose without loss of generality that the z_i are coprime and $z_i \neq 0$ for all $1 \leq i \leq n$. Indeed if $z_i = dz_i'$ where $d \in \mathbb{N}^*$ and $z_i' \in \mathbb{Z}$ with $\text{pgcd}(z_1', ..., z_n') = 1$, then it is equivalent to show that there are infinitely many primes dividing the $z_1^k + ... + z_n^k$ (for $k \geq 1$) or to show that there are infinitely many primes dividing the $(z_1')^k + ... + (z_n')^k$.

Under this assumption ($\text{pgcd}(z_1, ..., z_n) = 1$),the necessary and sufficient condition is :

$$(\exists i \in \{1, ..., n\} \text{ such that } |z_i| > 1) \text{ or } (n \text{ is even and } Card\{z_i = 1\} = Card\{z_i = -1\} = \tfrac{n}{2}).$$

Assume that $\exists i \in 1,...,n$ such that $|z_i| > 1$
In that case sequence $(S_{2k})_{k\geq 1} \longrightarrow +\infty$ when $k \longrightarrow +\infty$ (we took $2k$ because then the terms in S_{2k} are positives and there is no compensations between terms).
Let $G = \{p \in \mathbb{P} \mid \exists k \geq 1, \quad p \mid S_k\}$
Assume that G is finite and $G = \{p_1, ..., p_r\}$. Consider the subsequence $\left(S_{2\cdot\varphi(\prod_{i=1}^r p_i^\alpha)}\right)_{\alpha\geq 1}$ which also tends to $+\infty$. Then $\exists p \in G$ such that $\forall \alpha \geq 1, \forall N \geq 1, \exists k \geq N, \quad p^\alpha \mid S_{2\cdot\varphi(\prod_{i=1}^r p_i^k)}$.

Let $\beta \geq 1$ such that $p^\beta > n$ and α an integer such that $S_{2\cdot\varphi(\prod_{i=1}^r p_i^\alpha)} \equiv 0 \mod p^\beta$ and $2\cdot\varphi(\prod_{i=1}^r p_i^\alpha) \geq \beta$.
We have

$$\sum_{i=1}^n z_i^{2\cdot\varphi(\prod_{i=1}^r p_i^\alpha)} = \sum_{z_i\wedge p=1} z_i^{2\cdot\varphi(\prod_{i=1}^r p_i^\alpha)} + \sum_{z_i\wedge p\neq 1} z_i^{2\cdot\varphi(\prod_{i=1}^r p_i^\alpha)} \equiv n' \mod p^\beta$$

where n' is the number of $i \in \{1,...,n\}$ such that $z_i \wedge p = 1$. Then $n' \equiv 0 \mod p^\beta$, but $0 < n' \leq n < p^\beta$ ($n' \neq 0$ because the z_i are coprimes), and we obtain a contradiction. So G is not finite.

Secondly, if $\forall i \in \{1,...,n\}$, $|z_i| = 1$, then (S_k) is bounded, and the only way there could be infinitely many primes dividing this sequence is that there exists k such that $S_k = 0$. It is immediate that the necessary and sufficient condition is (n is even and $Card\{z_i = 1\} = Card\{z_i = -1\} = \frac{n}{2}$).

Question 3 (a). We find a necessary condition on the z_i : there must be a unique z_i of maximal modulus r, and $r \in \mathbb{N}^*$ (of course we assume that $z_i \neq 0$ for all i, otherwise it is the same problem with a smaller n). In particular if all the z_i are reals we find a necessary and sufficient condition which is : $n = 1$, $z_1 \in \mathbb{Z}$.

For the moment we don't assume that $z_i \in \mathbb{R}$. We suppose without loss of generality that $|z_1| \geq ... \geq |z_n| > 0$.

We suppose without loss of generality that $|z_1| \geq ... \geq |z_n|$ and we note $z_j = r_j * e^{2i\pi\alpha_j}$ where $r_j = |z_j|$. By hypothesis, we must have $S_k = \sum_{j=1}^n z_j^k = u_k^k$ for a sequence $(u_k)_{k\geq 1} \in \mathbb{Q}$. We write $u_k = \dfrac{a_k}{b_k}$ for some integers sequences such that $\forall k \geq 1, \quad a_k \wedge b_k = 1$. We have $b_k^k \cdot S_k = a_k^k$, and then it is immediate that b_k divides a_k (it suffices to look at the prime decomposition of b_k and a_k).

Let $r = max\,(|z_i|) = |z_1| > 0$, we have

$$u_k^k = \sum_{i=1}^n z_i^k = r^k * \sum_{i=1}^n \left(\frac{r_i}{r}\right)^k e^{2i\pi k\alpha_i}$$

Hence

$$|\frac{u_k}{r}|^k = |\sum_{i=1}^n \left(\frac{r_i}{r}\right)^k e^{2i\pi k\alpha_i}|$$

Using the triangle inequality, we obtain

$$|\sum_{i=1}^n \left(\frac{r_i}{r}\right)^k e^{2i\pi k\alpha_i}| \leq \sum_{i=1}^n \left(\frac{r_i}{r}\right)^k \leq n$$

Consequently, $\frac{|u_r|}{r} \leq n^{\frac{1}{k}}$. If $|u_k| > r$, then $|u_k| \geq E(r) + 1$ where $E(x)$ denotes the entire part of x, and $n^{\frac{1}{k}} \geq \frac{E(r)+1}{r} = Constant > 1$. But $n^{\frac{1}{k}} \to 1$ when $k \to +\infty$, and we conclude that :

$$\exists k_0,\ \forall k \geq k_0,\ |u_k| \leq r$$

which automatically leads to the stronger assertion :

$$\exists k_0,\ \forall k \geq k_0,\ |u_k| \leq E(r)$$

We are now able to solve the case : $\forall i \in \{1,...,n\},\ z_i \in \mathbb{R}$. We have $z_1 = \pm r$ and $n = 1$. Indeed, $u_{2k}^{2k} = S_{2k} = z_1^{2k} + ... + z_n^{2k} \geq r^{2k} \geq u_{2k}^{2k}$. Therefore the inequalities are equalities and $z_2 = ... = z_n = 0$, but we supposed $z_i \neq 0$, so $n = 1$ and $z_1 = \pm r \in \mathbb{Z}$ which is conversely a solution to the question.

We will show that in fact we can find arbitrarily large k such that the $k \cdot \alpha_j$ are simultaneously almost an integer. More precisely :

Lemma 1. *Let* $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{R}^n$. *Then* $\forall N > 1,\ \exists q \geq N$ *such that* $\exists (p_1, ..., p_n) \in \mathbb{N}^n, \quad \forall i \in \{1,...,n\}$

$$\left| \alpha_i - \frac{p_i}{q} \right| \leq \frac{1}{q^{1+\frac{1}{n}}}$$

Démonstration. If $\forall i \in \{1,...,n\},\ \alpha_i \in \mathbb{Q}$, then the lemma is obvious. So we can assume that for example $\alpha_1 \notin \mathbb{Q}$.

First of all, we change a bit the classical definition of the norm of a vector : if $\overrightarrow{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, then we define $||\overrightarrow{X}|| = max\,(|x_i|)$. Let $\overrightarrow{X} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ and $\overrightarrow{X_k} = k\overrightarrow{X} - E(\overrightarrow{kX})$ with $1 \leq k \leq N^n + 1$ (we use the following notation : if $\overrightarrow{X} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, then $E(\overrightarrow{X}) = \begin{pmatrix} E(\alpha_1) \\ \vdots \\ E(\alpha_n) \end{pmatrix}$). We share $[0,1]^n$ in N^n squares for an arbitrarily large integer $N > 1$. Using the box principle, we have :
$\exists i \neq j \in \{1, ..., N^n + 1\}, ||\overrightarrow{X_i} - \overrightarrow{X_j}|| \leq \dfrac{1}{N}$
i.e $||(i-j)\,\overrightarrow{X} - \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}|| \leq \dfrac{1}{N}$ for some $p_i \in \mathbb{Z}$.

Hence $\exists q_N \in \{1, ..., N^n\}$ and $p_i \in \mathbb{Z}$ such that $||q_N\overrightarrow{X} - \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}|| \leq \dfrac{1}{N} \leq \dfrac{1}{q_N^{\frac{1}{n}}}$ Now, let's prove that $(q_N)_{N\geq 1}$ is not a bounded sequence. If $(q_N)_{N\geq 1}$ was bounded, then it would contradict the fact that α_1 is irrational and therefore cannot be approximated arbitrarily close by rationals with bounded denominators.
The lemma is proved. □

Let m be the number of $i \in \{1,...,n\}$ such that $r_i = r_1 = r$ (recall that $r = r_1 = |z_1| \geq ... \geq |z_n| = r_n$). We apply the lemma to the vector $\overrightarrow{X} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. We can find $\phi : \mathbb{N}^* \to \mathbb{N}^*$ which is strictly increasing and such that $\forall k \geq 1, \forall i \in \{1,...,n\},\ \mid \phi(k)\alpha_i - p_i \mid \leq \frac{1}{\phi(k)^{1/n}}$. Then $|\sum_{i=1}^{n} \left(\frac{r_i}{r}\right)^{\phi(k)} e^{2i\pi\phi(k)\alpha_i}| \to m$ when $k \to +\infty$, because $e^{2i\pi\phi(k)\alpha_i} \to 1$. But we saw that for $\phi(k) \geq k_0$, $|\sum_{i=1}^{n} \left(\frac{r_i}{r}\right)^{\phi(k)} e^{2i\pi\phi(k)\alpha_i}| \leq 1$. Then $1 \leq m \leq 1$ and $m = 1$ (which means that $\forall i \geq 2,\ \mid z_1 \mid = r > r_i = \mid z_i \mid$). Furthermore, if for arbitrarily large k we have $\mid u_{\phi(k)} \mid < r$, then for these k, $\left(\mid \frac{u_{\phi(k)}}{r} \mid\right)^k \to 0$, wich contradict the fact that it tends to $m = 1$. Hence $\exists k_1 \geq 1,\ \forall k \geq k_1, u_{\phi(k)} = r$. In particular r is an integer.

Recall that $z_1 = r \cdot exp(2i\pi\alpha_1)$. We put $C = max\,(k_0, k_1)$. We have : $\forall k \geq C,\ u_{\phi(k)} = \pm r$ (the sign depends on k). We know that $exp(2i\pi \cdot \phi(k)\alpha_1) + \sum_{i=2}^{n} \left(\frac{z_i}{r}\right)^{\phi(k)} = \left(\frac{u_k}{r}\right)^{\phi(k)} = \pm 1$. At this point the only thing we can say is that everything depends on how well ca α_1 be approximated by rational numbers : if it can't be "well" approximated (i.e. here with an exponential speed), then there are no solutions (it is the case for example if α_1 is an algebraic integer).

0.1. **Question 3 (b).** We show in that question that a necessary condition is that all the same modulus $r \in \mathbb{N}^*$ and that the angle is a rational multiple of π. Furthermore we show that $\forall k \geq 0$, $S_k = 0$ or $\pm n$. In particular it leads to a necessary and sufficient condition on the z_i if we assume they are real numbers.

We assume without loss of generality that $|z_1| \geq ... \geq |z_n|$. Let $z_j = r_j exp(2i\pi\alpha_j)$, and $1 < r_i \leq r_j$ si $i \leq j$. By hypothesis we have $S_k = nu_k^k$ où $u_k \in \mathbb{Q}$. Because $S_k \in \mathbb{Z}$, for k large enough $u_k \in \mathbb{Z}$ (because if p is prime, $\frac{n}{p^k} \notin \mathbb{Z}$ for k large enough).

We rewrite the equation :

$$\sum_{j=1}^{n} \left(\frac{r_j}{r_1}\right)^k \cdot exp(2i\pi \cdot k\alpha_j) = n \cdot \left(\frac{u_k}{r_1}\right)^k$$

Like in question 3) a), because the left hand side is less or equal than n in modulus, we have $|u_k| \leq r_1$ for $k \geq k_0$. Furthermore the lemma in question 3) a) shows that the left hand side can be arbitrarily close to m, where $m = max\,(i \geq 1,\ r_i = r_1)$. So there exists $\phi : \mathbb{N}^* \to \mathbb{N}^*$ strictly increasing such that $\left|u_{\phi(k)}\right| = r_1$ (and r_1 is an integer). Then

$$\left|\sum_{j=1}^{n} \left(\frac{r_j}{r_1}\right)^{\phi(k)} \cdot exp(2i\pi \cdot \phi(k)\alpha_j)\right| = n$$

By letting $k \to +\infty$, we get $m = n$, i.e. all z_i have the same modulus r_1. In fact as we have $u_{\phi(k)} = \pm r_1$, then $\sum_{j=1}^{n} exp(2i\pi \cdot \phi(k)\alpha_j) = \pm n$, so $exp(2i\pi \cdot \phi(k)\alpha_j) = \epsilon$, for all $j \in \{1, ..., n\}$ for a $\epsilon \in \{-1, 1\}$. Hence we can write $\alpha_j = \frac{p_j}{q}$ for integers p_i et q.

In particular for all $k \geq 0$, $S_k = 0$ or $\pm n$. Indeed, for all $\epsilon > 0$, for k large enough, if $u_k \neq \pm 1$, then $n \cdot \left|\left(\frac{u_k}{r_1}\right)^k\right| < \epsilon$, wich is impossible for ϵ sufficiently small and $u_k \neq 0$ because $\frac{S_k}{r_1^k}$ takes a finite number of non zero values. But $\left(\frac{S_k}{r^k}\right)_{k \geq 1}$ is periodic and therefore for ALL $k \geq 0$, $S_k = 0$ or $\pm n$ (and not only for k large enough).

We don't have necessarily $q = 1$, because for example the z_i can be the vertex of a regular n-gone and it is a solution to the question.

We didn't find a necessary and sufficient condition in the general case, but we did some cases.

First if all the $z_i \in \mathbb{R}$, then $z_i = r \cdot \epsilon_i$ where $\epsilon_i \in \{-1, 1\}$, $r \in \mathbb{N}^*$. With the previous work, $\exists k_0,\ \forall k \geq k_0$, $\sum_{i=1}^{n} \epsilon_i^k = 0$ or n. This means that either $z_1 = ... = z_n \in \mathbb{Z}$, either half of the z_i is equal to r and the other half is equal to $-r$.

Now, with the previous notation, if q is prime and the z_i are not all equal, then q divides n and for all $0 \leq k < q$, there are exactly $\frac{n}{q}$ differents $i \in [1, n]$ such that $z_i = exp(2i\pi k/q)$ (i.e. the z_i forms n/q copies of the regular p-gone). Indeed, for $k = 1$, $z_1 + ... + z_n = 0$ or $\pm n$ (because if it was equal to $\pm n$, then all the z_i are equal), with $z_i = r \cdot exp(2i\pi\frac{p_i}{q})$ then if $\xi = \exp(2i\pi/q)$, we have a polynomial equation $n_0 + n_1\xi + n_2\xi^2 + ... + n_{q-1}\xi^{q-1} = 0$ with $n_i = Card(\{j \in \{1, ..., n\}, z_j = \xi^i\})$. Classical results on the q-th cyclotomic polynomial implie that $n_0 = n_1 = ... = n_{q-1}$, and we have the desired result.

1. Appendix

For theorems about rings of integers and algebraic integers, see Pierre Samuel, Théorie algébrique des nombres, Chapter II, III, IV.