GENERALIZATION OF A POHST'S INEQUALITY

FRANCESCO BATTISTONI AND GIUSEPPE MOLTENI

Abstract. Let

$$P_n(y_1,\dots,y_n) \coloneqq \prod_{1\le i<j\le n}\left(1-\frac{y_i}{y_j}\right)$$

and

$$P_n \coloneqq \sup_{(y_1,\dots,y_n)} P_n(y_1,\dots,y_n)$$

where the supremum is taken over the n-ples $(y_1,\dots,y_n)$ of real numbers satisfying $0<|y_1|<|y_2|<\cdots<|y_n|$. We prove that $P_n \le 2^{\lfloor n/2\rfloor}$ for every n, i.e., we extend to all n the bound that Pohst proved for $n\le 11$. As a consequence, the bound for the absolute discriminant of a totally real field in terms of its regulator is now proved for every degree of the field.

J. Number Th. **228**, 73–86 (2021).
DOI: https://doi.org/10.1016/j.jnt.2021.04.014

1. Introduction

Let $y_1,\dots,y_n$ be $n\ge 2$ non zero real numbers satisfying the condition

$$|y_1|<|y_2|<\cdots<|y_n|. \tag{1}$$

Define then the positive real number

$$P_n(y_1,\dots,y_n) \coloneqq \prod_{1\le i<j\le n}\left(1-\frac{y_i}{y_j}\right)$$

and consider

$$P_n \coloneqq \sup_{(y_1,\dots,y_n)} P_n(y_1,\dots,y_n),$$

where the supremum is taken over the n-ples of real numbers $(y_1,\dots,y_n)$ which satisfy the condition (1).

The goal of this paper is to provide an estimation for P_n for every $n\ge 2$. This is motivated by number theoretic reasons: in fact, let K be a number field of degree $n\ge 2$ and let ε be a unit of its ring of integers such that $K=\mathbb{Q}(\varepsilon)$. The discriminant d_K of the field K divides the discriminant of the minimum polynomial of ε, inducing the inequality

$$|d_K| \le \prod_{1\le i<j\le n}|\varepsilon_i-\varepsilon_j|^2 \le \prod_{k=2}^{n}|\varepsilon_k|^{2(k-1)}\cdot\prod_{1\le i<j\le n}\left(1-\frac{\varepsilon_i}{\varepsilon_j}\right)^2 \le \prod_{k=2}^{n}|\varepsilon_k|^{2(k-1)}\cdot P_n^2.$$

Furthermore, when K is totally real and primitive (i.e. has no proper subfields) it is possible to estimate the remaining product in terms of the regulator R_K of K with classical methods from geometry of numbers (for example see [1]), and one obtains that

$$\log|d_K| \le \sqrt{\gamma_{n-1}\cdot\frac{n^3-n}{3}}\cdot(\sqrt{n}R_K)^{1/(n-1)} + 2\log P_n,$$

where γ_{n-1} denotes the Hermite constant of dimension $n-1$ (for the definition of this constant see [4, Ch. 3, Sec. 3]). Thus, any estimation for P_n provides an estimation for the discriminant d_K. More precisely, Remak [5] first showed that $P_n\le n^{n/2}$ for every n; Pohst [3] improved the bound to $P_n\le 2^{\lfloor n/2\rfloor}$ for every $n\le 11$, and Bertin [2] produced a new proof of Remak's estimate. In the same paper Bertin also gave an argument trying to prove that Pohst's estimation holds

2010 *Mathematics Subject Classification.* 11R80, 11Y40.

Key words and phrases. Totally real fields, explicit bounds.

The first author was supported by the French "Investissements d'Avenir" program, project ISITE-BFC (contract ANR-lS-IDEX-OOOB).

for every n, but her procedure is not completely convincing. In this paper we prove that Pohst's estimation holds indeed for every n.

In order to achieve this result, following aforementioned works, we choose a slightly different function to estimate: given $P_n(y_1,\dots,y_n)$, we define the change of variables

$$x_i \coloneqq \frac{y_i}{y_{i+1}}, \qquad i=1,\dots,n-1 \tag{2}$$

which transforms $P_n(y_1,\dots,y_n)$ into the quantity

$$Q_{n-1}(x_1,\dots,x_{n-1}) \coloneqq \prod_{i=1}^{n-1}\prod_{j=i}^{n-1}\left(1-\prod_{k=i}^{j}x_k\right).$$

Since $|x_i|\le 1$ for every i, the polynomials Q_n are non negative over the cube $D_n \coloneqq [-1,1]^n$, and we look for

$$M_n \coloneqq \max_{(x_1,\dots,x_n)\in D_n} Q_n(x_1,\dots,x_n).$$

The change of variables (2) shows that $P_n = M_{n-1}$ for every $n\ge 2$. Starting from this, in the next sections we will prove the following theorem.

Theorem 1. *The maximum M_n of Q_n in D_n is $2^{\lfloor \frac{n+1}{2}\rfloor}$ for every n, so that $P_n = M_{n-1} = 2^{\lfloor n/2\rfloor}$ for every $n\ge 2$.*

It is easy to verify that Q_n attains its maximum at $(-1,0,-1,0,\dots)$ when n is odd, while for an even n this happens at each point $([-1,0]^k,[0,-1]^{n/2-k})$ for any choice of $k=0,1,\dots,n/2$ (here $[-1,0]^k$ means that the string $[-1,0]$ has to be repeated k times, the same for $[0,-1]^{n/2-k}$). Our argument proving Theorem 1 can be adapted to prove also that these are the unique points where Q_n attains its maximum, but we leave to the interested reader a formal proof of this fact.

Corollary 1. *Let K be a totally real and primitive field of degree $n\ge 2$ having discriminant d_K and regulator R_K. Then*

$$\log|d_K| \le \sqrt{\gamma_{n-1}\cdot\frac{n^3-n}{3}}\cdot(\sqrt{n}R_K)^{1/(n-1)} + \left\lfloor\frac{n}{2}\right\rfloor\log 4.$$

2. Basic inequalities

An elementary computation shows that the maximums for the first two polynomials $Q_1(x_1) = (1-x_1)$ and $Q_2(x_1,x_2) = (1-x_1)(1-x_1x_2)(1-x_2)$ are

$$M_1 = 2, \qquad M_2 = 2, \tag{3}$$

respectively. These numbers agree with the claim of the theorem. It is clear that the determination of M_n via local, i.e. analytic, methods involving partial derivatives becomes quickly infeasible as n increases: we take a different and global, so to say, approach, where the polynomial is split in suitable blocks and the maximum for the polynomial is deduced from the maximums of those blocks. These maximums will be deduced from the following basic inequalities.

Lemma 1. *Let x,y,z be real numbers in $[0,1]$. Then the following inequalities hold:*

$$(1-x)(1+xy)\le 1, \tag{4}$$

$$(1-x)(1+xy)\le(1+x)(1-xy), \tag{5}$$

$$(1-y)(1+xy)(1+yz)(1-xyz)\le(1+y)(1-xy)(1-yz)(1+xyz), \tag{6}$$

$$(1-y)(1+xy)(1+yz)(1-xyz)\le 1. \tag{7}$$

Proof. (4) is obvious, since $1+xy\le 1+x$. (5) is reduced via direct computations to $-x+xy\le 0$, which is clearly true. For (6): the right hand side minus the left hand side factorizes as

$$2y(1-x)(1-z)(1+xy^2z),$$

which is nonnegative under our hypotheses.
Finally, (7) already appears in [3]; for sake of completeness we recall here a quicker proof. Compute all the products, remove the common terms, factor out y and move the terms to left

hand side or right hand side according to the sign of the coefficient. In this way the inequality is proved to be equivalent to

$$(y^3z^2+y^2z)x^2+(y^2z^2+yz+1)x+xyz+z\le(y^2z^2+yz)x^2+(y^2z+yz^2+y+z)x+yz+1.$$

This inequality is true since it can be obtained adding the three inequalities

$$x^2y^3z^2+x^2y^2z+xy^2z^2\le x^2y^2z^2+x^2yz+xy^2z,$$
$$x+y+z+xyz\le xy+xz+yz+1,$$
$$xyz-y\le xyz^2$$

which are true (the first one because each term appearing to the left contains and extra power with respect to the corresponding term to the right, the second one because it can be written as $(1-x)(1-y)(1-z)\ge 0$, and the last one because $y(1-xz+xz^2)\ge 0$ in the given range). □

3. Graphical schemes

We call *graphical scheme of dimension n* any triangular $n\times n$ array C with symbols "+" or "−" in each entry $C_{i,j}$ with $1\le i\le j\le n$. The following are some examples of graphical schemes in dimension $n=3$ and $n=5$, respectively:

+	+	−
	−	+
		+

,

−	−	+	+	−
	+	−	−	+
		+	+	−
			−	−
				−

.

We associate with C the function $F_C\colon[0,1]^n\to\mathbb{R}$ defined as

$$F_C(z_1,\dots,z_n)\coloneqq\prod_{i=1}^{n}\prod_{j=i}^{n}\left(1-C_{i,j}\prod_{k=i}^{j}z_k\right),$$

and we denote its (i,j) factor as

$$F_{C_{i,j}}\coloneqq 1-C_{i,j}\prod_{k=i}^{j}z_k.$$

Given two graphical schemes C and C' of dimension n, we say that $C\le C'$ if $F_C(z_1,\dots,z_n)\le F_{C'}(z_1,\dots,z_n)$ for every choice of $(z_1,\dots,z_n)\in[0,1]^n$. The following lemma describes four basic moves that when performed on a given scheme produce a larger (in the previous sense) scheme.

Lemma 2. *Let C be a graphical scheme of dimension n.*

*P) (**Point**) Assume $C_{i,j}=+$. Let C' be the graphical scheme defined by*

$$C'_{r,s}=\begin{cases}-&(r,s)=(i,j)\\ C_{r,s}&\text{otherwise.}\end{cases}$$

Then $C\le C'$. Moreover, $F_{C_{i,j}}\le 1$.

*H) (**Horizontal segment**) Assume $C_{i,j}=+$ and $C_{i,j+k}=-$, with $k\le n-j$. Let C' be the graphical scheme defined by*

$$C'_{r,s}=\begin{cases}-&(r,s)=(i,j)\\ +&(r,s)=(i,j+k)\\ C_{l,k}&\text{otherwise.}\end{cases}$$

Then $C\le C'$. Moreover, $F_{C_{i,j}}\cdot F_{C_{i,j+k}}\le 1$.

V) (***Vertical segment***) *Assume* $C_{i,j} = -$ *and* $C_{i+k,j} = +$ *with* $k \leq j - i$. *Let* C' *be the graphical scheme defined by*

$$C'_{r,s} = \begin{cases} + & (r,s) = (i,j) \\ - & (r,s) = (i+k,j) \\ C_{l,k} & \textit{otherwise.} \end{cases}$$

Then $C \leq C'$. *Moreover,* $F_{C_{i,j}} \cdot F_{C_{i+k,j}} \leq 1$.

S) (***Square***) *Assume* $C_{i,j} = -, C_{i,j+k} = +, C_{i+l,j} = +$ *and* $C_{i+l,j+k} = -$. *Let* C' *be the graphical scheme defined by*

$$C'_{r,s} = \begin{cases} + & (r,s) = (i,j) \\ - & (r,s) = (i,j+k) \\ - & (r,s) = (i+l,j) \\ + & (r,s) = (i+l,j+k) \\ C_{l,k} & \textit{otherwise.} \end{cases}$$

Then $C \leq C'$. *Moreover,* $F_{C_{i,j}} F_{C_{i+l,j}} F_{C_{i,j+k}} F_{C_{i+l,j+k}} \leq 1$.

We introduce a notation for these moves:

P) **Point**: $\mathrm{P}(i;j)$ denotes the change of $\begin{smallmatrix} & j \\ i & \boxed{+} \end{smallmatrix}$ into $\begin{smallmatrix} & j \\ i & \boxed{-} \end{smallmatrix}$,

H) **Horizontal**: $\mathrm{H}(i;j,j')$ denotes the change of $\begin{smallmatrix} & j & j' \\ i & \boxed{+}\boxed{-} \end{smallmatrix}$ into $\begin{smallmatrix} & j & j' \\ i & \boxed{-}\boxed{+} \end{smallmatrix}$,

V) **Vertical**: $\mathrm{V}(i,i';j)$ denotes the change of $\begin{smallmatrix} & j \\ i & \boxed{-} \\ i' & \boxed{+} \end{smallmatrix}$ into $\begin{smallmatrix} & j \\ i & \boxed{+} \\ i' & \boxed{-} \end{smallmatrix}$,

S) **Square**: $\mathrm{S}(i,i';j,j')$ denotes the change of $\begin{smallmatrix} & j & j' \\ i & \boxed{-}\boxed{+} \\ i' & \boxed{+}\boxed{-} \end{smallmatrix}$ into $\begin{smallmatrix} & j & j' \\ i & \boxed{+}\boxed{-} \\ i' & \boxed{-}\boxed{+} \end{smallmatrix}$.

Proof.

P) We have

$$F_{C_{i,j}} = 1 - \prod_{k=i}^{j} z_k \leq 1 + \prod_{k=i}^{j} z_k$$

and since every other factor of F_C remains unchanged, we get $F_C \leq F_{C'}$. The statement $F_{C_{i,j}} \leq 1$ is immediate.

H) $F_{C_{i,j}} \cdot F_{C_{i,j+k}} \leq 1$ is a direct consequence of (4), while (5) implies

$$\begin{aligned} F_{C_{i,j}} \cdot F_{C_{i,j+k}} &= \left(1 - \prod_{l=i}^{j} z_l\right)\left(1 + \prod_{l=i}^{j} z_l \prod_{l=j+1}^{j+k} z_l\right) \\ &\leq \left(1 + \prod_{l=i}^{j} z_l\right)\left(1 - \prod_{l=i}^{j} z_l \prod_{l=j+1}^{j+k} z_l\right) = F_{C'_{i,j}} \cdot F_{C'_{i,j+k}} \end{aligned}$$

and this proves $F_C \leq F_{C'}$ since every other factor is unchanged.

V) is proved in a similar way to case H).

S) $F_{C_{i,j}} F_{C_{i+l,j}} F_{C_{i,j+k}} F_{C_{i+l,j+k}} \leq 1$ is a direct application of (7), while (6) implies

$$\begin{aligned} &F_{C_{i+l,j}} \cdot F_{C_{i,j}} \cdot F_{C_{i+l,j+k}} \cdot F_{C_{i,j+k}} \\ &= \left(1 - \prod_{v=i+l}^{j} z_v\right)\left(1 + \prod_{v=i}^{i+l-1} z_v \prod_{v=i+l}^{j} z_v\right)\left(1 + \prod_{v=i+l}^{j} z_v \prod_{v=j+1}^{j+k} z_v\right)\left(1 - \prod_{v=i}^{i+l-1} z_v \prod_{v=i+l}^{j} z_v \prod_{v=j+1}^{j+k} z_v\right) \\ &\leq \left(1 + \prod_{v=i+l}^{j} z_v\right)\left(1 - \prod_{v=i}^{i+l-1} z_v \prod_{v=i+l}^{j} z_v\right)\left(1 - \prod_{v=i+l}^{j} z_v \prod_{v=j+1}^{j+k} z_v\right)\left(1 + \prod_{v=i}^{i+l-1} z_v \prod_{v=i+l}^{j} z_v \prod_{v=j+1}^{j+k} z_v\right) \\ &= F_{C'_{i+l,j}} \cdot F_{C'_{i,j}} \cdot F_{C'_{i+l,j+k}} \cdot F_{C'_{i,j+k}} \end{aligned}$$

and this proves $F_C \leq F_{C'}$ since every other factor is unchanged.

□

4. Properties of the schemes generated by sign vectors

Identifying numbers ± 1 with symbols $\pm$, we can generate a graphical scheme $C(\boldsymbol{\varepsilon})$ from each signs vector $\boldsymbol{\varepsilon} \coloneqq (\varepsilon_1, \dots, \varepsilon_n)$, $\varepsilon_k \in \{\pm 1\}$, by setting $C(\boldsymbol{\varepsilon})_{i,j} \coloneqq \prod_{k=i}^{j} \varepsilon_k$ for every (i, j). For example, the vector $\boldsymbol{\varepsilon} \coloneqq (1, 1, -1, 1, -1)$ generates the scheme

$C(\boldsymbol{\varepsilon}) =$

+	+	−	−	+
	+	−	−	+
		−	−	+
			+	−
				−

The interest for this construction comes from the following remark. We can split $D_n = [-1, 1]^n$ into 2^n different chambers $D_{n,\boldsymbol{\varepsilon}}$, each one associated with a different signs vector $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$, where

$$D_{n,\boldsymbol{\varepsilon}} \coloneqq \{(x_1, \dots, x_n) \in [-1, 1]^n \colon x_i \varepsilon_i \geq 0,\ \forall i\}.$$

Once we have chosen $D_{n,\boldsymbol{\varepsilon}}$, the change of variables $z_i \coloneqq \varepsilon_i x_i$ transforms $D_{n,\boldsymbol{\varepsilon}}$ into $[0, 1]^n$, and $Q_n(x_1, \dots, x_n)$ into

$$Q_n(\varepsilon_1 z_1, \dots, \varepsilon_n z_n) = \prod_{i=1}^{n} \prod_{j=i}^{n} \left(1 - \prod_{k=i}^{j} \varepsilon_k \prod_{k=i}^{j} z_k\right),$$

which is exactly the polynomial $F_{C(\boldsymbol{\varepsilon})}$ associated with the scheme $C(\boldsymbol{\varepsilon})$ generated by the signs vector $\boldsymbol{\varepsilon}$. This gives us a strategy to prove Theorem 1: we will prove that for each scheme $C(\boldsymbol{\varepsilon})$ there is a list of moves P, V, H and S which transform $C(\boldsymbol{\varepsilon})$ into C_-, the n-dimensional scheme generated by the signs $\boldsymbol{\varepsilon}_- \coloneqq (-1, \cdots, -1)$ (see next Theorem 2): by Lemma 2 these moves increase the value of the associated polynomial, hence the maximum of each $F_{C(\boldsymbol{\varepsilon})}$ is lower than the one of F_{C_-}. In other words, this means that the maximum of Q_n in every chamber $D_{n,\boldsymbol{\varepsilon}}$ is the one of F_{C_-}, at most. Thus, the conclusion easily follows from the next lemma giving the maximum for F_{C_-}.

Lemma 3. *Let C_- be the n-dimensional scheme generated by the signs $\boldsymbol{\varepsilon}_- \coloneqq (-1, \cdots, -1)$. Then*

$$F_{C_-}(z_1, \dots, z_n) \leq 2^{\left\lfloor \frac{n+1}{2} \right\rfloor} \qquad \forall (z_1, \dots, z_n) \in [0, 1]^n.$$

Proof. The graphical scheme C_- has the form

−	+	−	+	⋯
	−	+	−	⋯
		−	+	⋯
			−	⋯
				⋯

where every row starts with a sign $-$ and continues with alternating signs. We know that the claim for $n = 1$ and $n = 2$ is true thanks to (3). Let $n \geq 3$. If n is odd, the scheme C_- has the form

−	+	−	+	⋯	−	+	−
	−	+	−	⋯	+	−	+

$C_{-,n-2}$

while for n even has the form

−	+	−	+	⋯	−	+
	−	+	−	⋯	+	−

$C_{-,n-2}$

where in both cases $C_{-,n-2}$ is the $n-2$-dimensional scheme defined by the $n-2$-long vector with all minus signs. By inductive hypothesis, we have $F_{C_{-,n-2}} \leq 2^{\lfloor (n-1)/2 \rfloor}$.
Let us look at the first two rows of C_-: here, the first two columns form a triangular array in dimension 2: hence $F_{C_{1,1}} F_{C_{1,2}} F_{C_{2,2}} \leq 2$ by Equation (3). Moreover, there are $\lfloor (n-2)/2 \rfloor$ consecutive squares $\begin{array}{|c|c|}\hline - & + \\ \hline + & - \\ \hline \end{array}$, plus, in case n is odd, an extra vertical segment $\begin{array}{|c|}\hline - \\ \hline + \\ \hline \end{array}$. Entries V) and S) of Lemma 2 prove that the contribution of each such square and of the vertical segment are bounded by 1. Hence, in every case the contribution of the first two rows is estimated by 2, and

$$F_{C_-} \leq 2 \cdot F_{C_{-,n-2}} \leq 2 \cdot 2^{\lfloor \frac{n-1}{2} \rfloor} = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

□

To succeed in this task we need to further investigate some properties of the schemes generated by sign vectors; they are contained in next three lemmas.

Lemma 4. *Let $C(\boldsymbol{\varepsilon})$ be a scheme generated by the sign vector $\boldsymbol{\varepsilon}$ of dimension $n \geq 3$. Let $i < i'$, $j < j'$ with $i' < j$. The product of the four signs $C(\boldsymbol{\varepsilon})_{i,j}$, $C(\boldsymbol{\varepsilon})_{i',j}$, $C(\boldsymbol{\varepsilon})_{i,j'}$ and $C(\boldsymbol{\varepsilon})_{i',j'}$ is 1. In other words, the number of minus signs in every square $\begin{array}{c} \\ i \\ i' \end{array}\!\!\begin{array}{cc} j & j' \\ \square & \square \\ \square & \square \end{array}$ is even.*

Proof. In fact, we have

$$C(\boldsymbol{\varepsilon})_{i,j} C(\boldsymbol{\varepsilon})_{i',j} C(\boldsymbol{\varepsilon})_{i,j'} C(\boldsymbol{\varepsilon})_{i',j'} = \prod_{k=i}^{j} \varepsilon_k \prod_{k=i'}^{j} \varepsilon_k \prod_{k=i}^{j'} \varepsilon_k \prod_{k=i'}^{j'} \varepsilon_k = \prod_{k=j+1}^{j'} \varepsilon_k \prod_{k=j+1}^{j'} \varepsilon_k = 1.$$

□

Let C be a graphical scheme. We say that the sign $C_{i,j}$ is *correct* if $C_{i,j} = (-1)^{i-j+1}$, otherwise we say that $C_{i,j}$ is *wrong*. It is clear that the only graphical scheme having only correct signs is C_-, i.e., the one generated by the signs vector $\boldsymbol{\varepsilon}_- := (-1, \ldots, -1)$.

Lemma 5. *Let $C(\boldsymbol{\varepsilon})$ be a scheme generated by the sign vector $\boldsymbol{\varepsilon}$ of dimension n and for $i \leq j \leq n$ let $H(i,j) := \sum_{u=i}^{j-1} C(\boldsymbol{\varepsilon})_{i,u}$ (the sum of entries in $C(\boldsymbol{\varepsilon})$ appearing to the left of $C(\boldsymbol{\varepsilon})_{i,j}$), and $V(i,j) := \sum_{v=i+1}^{j} C(\boldsymbol{\varepsilon})_{v,j}$ (the sum of entries in $C(\boldsymbol{\varepsilon})$ appearing below $C(\boldsymbol{\varepsilon})_{i,j}$). Suppose that $C(\boldsymbol{\varepsilon})_{i,j} = -$, then $H(i,j) = -V(i,j)$.*

Proof. In fact, $C(\boldsymbol{\varepsilon})_{i,u} = \prod_{k=i}^{u} \varepsilon_k$ and by hypothesis $C(\boldsymbol{\varepsilon})_{i,j} = \prod_{k=i}^{j} \varepsilon_k = -1$. Thus, for $i \leq u \leq j-1$ we get

$$C(\boldsymbol{\varepsilon})_{i,u} = \prod_{k=i}^{u} \varepsilon_k = -C(\boldsymbol{\varepsilon})_{i,j} \prod_{k=i}^{u} \varepsilon_k = -\prod_{k=i}^{j} \varepsilon_k \prod_{k=i}^{u} \varepsilon_k = -\prod_{k=u+1}^{j} \varepsilon_k = -C(\boldsymbol{\varepsilon})_{u+1,j}.$$

Hence, each term appearing below $C(\boldsymbol{\varepsilon})_{i,j}$ is opposite to a convenient term appearing to the left of $C(\boldsymbol{\varepsilon})_{i,j}$, and vice versa. □

We introduce the following quantities, again under the hypothesis that $i \leq j$.

$$H^w_{\pm}(i,j) := \#\{k \colon i \leq k \leq j-1, C_{i,k} = \pm, C_{i,k} \text{ is wrong}\},$$
$$V^w_{\pm}(i,j) := \#\{k \colon i+1 \leq k \leq j, C_{k,j} = \pm, C_{k,j} \text{ is wrong}\},$$
$$H^w(i,j) := H^w_+(i,j) - H^w_-(i,j), \qquad V^w(i,j) := V^w_+(i,j) - V^w_-(i,j).$$

Lemma 6. *Let $C(\boldsymbol{\varepsilon})$ be a scheme generated by the sign vector $\boldsymbol{\varepsilon}$ and assume that $C(\boldsymbol{\varepsilon})_{i,j} = -$ and that $i+j$ is odd. Then $V(i,j) = 2V^w(i,j) - 1$ and $H(i,j) = 2H^w(i,j) - 1$. We know that $V(i,j)$ and $H(i,j)$ are opposite in sign by Lemma 5, therefore $H^w(i,j) + V^w(i,j) = 1$ and in particular, at least one between $H^w(i,j)$ and $V^w(i,j)$ is positive.*

Proof. Since $i+j$ is odd, there exist $j-i$ signs $C(\boldsymbol{\varepsilon})_{l,j}$ below $C(\boldsymbol{\varepsilon})_{i,j}$, and the quantity $j-l+1$ is odd for $(j-i+1)/2$ of them, and is even for the remaining $(j-i-1)/2$ cases. Wrong $+$'s

below $C(\boldsymbol{\varepsilon})_{i,j}$ appear at positions (l,j) where $j-l+1$ is odd, and every other sign here which is not a wrong $+$ is necessarily a $-$ (actually a correct $-$, but this in not important now), thus

$$\sum_{\substack{l=i+1\\ j-l+1\,\text{odd}}}^{j} C(\boldsymbol{\varepsilon})_{l,j} = V_+^w(i,j) - \Big(\frac{1}{2}(j-i+1) - V_+^w(i,j)\Big) = 2V_+^w(i,j) - \frac{1}{2}(j-i+1).$$

Similarly, wrong $-$'s below $C(\boldsymbol{\varepsilon})_{i,j}$ appear at positions (l,j) where $j-l+1$ is even, and every other sign here which is not a wrong $-$ is necessarily a $+$, so that

$$\sum_{\substack{l=i+1\\ j-l+1\,\text{even}}}^{j} C(\boldsymbol{\varepsilon})_{l,j} = -V_-^w(i,j) + \Big(\frac{1}{2}(j-i-1) - V_-^w(i,j)\Big) = -2V_-^w(i,j) + \frac{1}{2}(j-i-1)$$

Thus

$$V(i,j) = \sum_{l=i+1}^{j} C(\boldsymbol{\varepsilon})_{l,j} = 2(V_+^w(i,j) - V_-^w(i,j)) - \frac{1}{2}(j-i+1) + \frac{1}{2}(j-i-1) = 2V^w(i,j) - 1.$$

The proof for $H(i,j)$ is similar. □

5. The procedure

We are now ready to prove the following theorem. As recalled in the previous section, it yields Theorem 1 as immediate corollary thanks to Lemma 2 and Lemma 3.

Theorem 2. *Let $C = C(\boldsymbol{\varepsilon})$ be the scheme generated by any signs vector $\boldsymbol{\varepsilon}$ and let C_- be the scheme generated by the sign vector $\boldsymbol{\varepsilon}$ with all negative signs. There is a list $\mathcal{L}$ of transformations of type* P*,* H*,* V *and* S *which changes C into C_-.*

Proof. Let $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$ be the signs vector producing C. We prove the theorem by making induction on the dimension n.
If $n = 1$, we only have two possibilities: either $C = \boxed{-}$ and we have finished, or $C = \boxed{+}$ and the claim follows by applying P(1; 1).
Now, assume that $n > 1$ and that the claim is true for every scheme generated by any signs pattern of dimension less than n. Let C' be the scheme obtained by removing the n-th column from C: this is the scheme generated by the signs vector omitting ε_n in $\boldsymbol{\varepsilon}$. By inductive hypothesis, there exists a list $\mathcal{L}'$ of moves which applied to C' gives C'_-, the array of dimension $n-1$ defined by all negative signs. Our goal is to modify some elements in $\mathcal{L}'$ by replacing them with other moves which correct all wrong symbol in the n-th column and that coincide with the old move on the common part in C': in this way we will obtain a new list $\mathcal{L}$ of moves that applied to C give C_-.
Moreover, in order to prove that the algorithm can be correctly performed, we need to keep note of each move we introduce, and of its effect on the n-th column. For this purpose we introduce the symbols $D_{(1)}$, $D_{(2)}$ and so on, to denote the several new versions of the n-th column we get after each new move is performed. At the beginning we have $D_{(1)}$, which coincides with the n-th column in C.
We start running the column $D_{(k)}$ from the bottom to the top, looking for wrong signs $-$. In case such signs do not appear, we skip this step and we go directly to the last one. On the contrary, suppose that we have found a *wrong* $-$ in i-th line. We will see that in each new version of the column only some wrong positions are changed with respect to its previous version. As a consequence, the *wrong* $-$ in line i-th we have detected now was already there at the beginning, i.e., $C_{i,n} = -$ and $i+n$ is odd. We compute both $V^w(i,n)$ and $V^w_{\text{new}}(i,n)$, which are the sum of *wrong* signs appearing below the (i,n) position respectively in C, the original scheme, and in the column $D_{(k)}$: at the beginning evidently numbers $V^w(i,n)$ and $V^w_{\text{new}}(i,n)$ coincide, but as the algorithm progresses the second may change its value. However, we will check that after each move we will introduce is executed, the value of the index

$$\big[\text{number of } \textit{wrong } + \text{ below } l \text{ in } n\text{-th column}\big] - \big[\text{number of } \textit{wrong } - \text{ below } l \text{ in } n\text{-th column}\big]$$

for each $l < i$ does not decrease. This proves that the number $V^w_{\text{new}}(i,n)$ we compute in any time is for sure $\geq V^w(i,n)$.

We note that the number $V(i,n)$ is odd, by Lemma 6. In particular, it cannot be 0.

Suppose that $V(i,n) > 0$. Then $V^w(i,n) > 0$ by Lemma 6, and $V^w_{\text{new}}(i,n)$ is positive as well by the previous remark. This means that in some position below (i,n) there is a *wrong* $+$ in column n. Let i' be the first (i.e., smallest) index $i' > i$ such that in the (i',n) position there is a wrong $+$. We add to $\mathcal{L}'$ the move $\mathrm{V}(i,i';n)$: this move is independent of the other moves, and converts the wrong $-$ and $+$ in those positions into two correct symbols. This move does not change the value of

$$\big[\text{number of } \textit{wrong} + \text{ below } l \text{ in } n\text{-th column}\big] - \big[\text{number of } \textit{wrong} - \text{ below } l \text{ in } n\text{-th column}\big]$$

for each $l < i$, because the move simply exchanges a $+$ with a $-$ both in positions below the l-th position.

Suppose that $V(i,n) < 0$. Then $V^w(i,n) < 0$ and $H^w(i,n)$ is positive, both by Lemma 6. Thus, in the i-th horizontal line to the left of $C_{i,n}$, and hence in C', there is an excess of *wrong* $+$'s with respect to *wrong* $-$'s. By induction there are moves in $\mathcal{L}'$ changing all these *wrong* entries. Moves of type H or S cannot be the unique moves in $\mathcal{L}'$ affecting these positions, since they exchange both a *wrong* $+$ and a *wrong* $-$ and therefore cannot remove the excess. Also a move of type $\mathrm{V}(i,i';j)$ $\begin{array}{c} \\ i \\ i' \end{array}\!\!\begin{array}{|c|}\hline j \\ \hline - \\ \hline + \\ \hline \end{array}$ is not sufficient to remove the excess, since it removes only a *wrong* $-$ from that line, a fact which actually increases the excess. Thus, at least a move $\mathrm{P}(i;j)$ $\begin{array}{c} \\ i \end{array}\!\!\begin{array}{|c|}\hline j \\ \hline + \\ \hline \end{array}$ or a move $\mathrm{V}(i',i;j)$ $\begin{array}{c} \\ i' \\ i \end{array}\!\!\begin{array}{|c|}\hline j \\ \hline - \\ \hline + \\ \hline \end{array}$ is in $\mathcal{L}'$. Let us take j to be the greatest index $< n$ such that this happens. In the first case we substitute $\mathrm{P}(i;j)$ with $\mathrm{H}(i;j,n)$ $\begin{array}{c} \\ i \end{array}\!\!\begin{array}{|c|c|}\hline j & n \\ \hline + & - \\ \hline \end{array}$ which has the same effect on the C' part of the configuration. In the second case we note that the signs at (i',j), (i,j) and (i,n) positions are $\begin{array}{c} \\ i' \\ i \end{array}\!\!\begin{array}{|c|c|}\hline j & n \\ \hline - & \\ \hline + & - \\ \hline \end{array}$. By Lemma 4 the fourth corner $C_{i',n}$ of the square in C is a *wrong* $+$. We will show in a moment that this is a $+$ also in $D_{(k)}$, i.e. it appears also at this stage of the algorithm. Letting this fact for granted for the moment, we proceed substituting $\mathrm{V}(i',i;j)$ in $\mathcal{L}'$ with $\mathrm{S}(i',i;j,n)$ $\begin{array}{c} \\ i' \\ i \end{array}\!\!\begin{array}{|c|c|}\hline j & n \\ \hline - & + \\ \hline + & - \\ \hline \end{array}$ which again has the same effect on the C' part of the configuration. Both moves change

$$\big[\text{number of } \textit{wrong} + \text{ below } l \text{ in } n\text{-th column}\big] - \big[\text{number of } \textit{wrong} - \text{ below } l \text{ in } n\text{-th column}\big]$$

in positions $l < i$. However, the first one actually simply removes a *wrong* $-$, so that it increases the index for all $l < i$, while the second one increases it when $i' \le l < i$ (because it removes the *wrong* $-$), and keeps unchanged its value for $l < i'$ (because then also the cancellation of the *wrong* $+$ at $C_{i',n}$ matters).
We execute the move we have selected, getting the new column which is $D_{(k+1)}$, by definition. We repeat this cycle again and again, removing all *wrong* $-$'s from the n-column in C. Finally, we add P moves to $\mathcal{L}'$ to remove any remaining *wrong* $+$'s in last column, if any exists.

The description of the algorithm ends here, but we have to resume the point we have skipped before, i.e., the proof of the fact that the *wrong* $+$ appearing at the fourth corner (i',n) of the square in C also appears in $D_{(k)}$, i.e. it appears also at that stage of the algorithm. Suppose the contrary, i.e., that the *wrong* $+$ is no more there, since it has been corrected at some earlier step of the algorithm. Then, there had been some index $i'' > i$ with $C_{i'',n} = -$ whose correction needed the substitution of some move $\mathrm{V}(i',i'';j')$ in $\mathcal{L}'$ with $\mathrm{S}(i',i'';j',n)$ for some $j' \neq j$, because this is the only possible way the algorithm can correct the $+$ at (i',n) at some previous step (the case $j' = j$ is for sure impossible, otherwise the *wrong* $-$ at (i',j') would be corrected in that previous step and would not be available at k-th step). This means that we have one of the following signs patterns in C:

$$\begin{array}{c} \\ i' \\ i \\ i'' \end{array}\!\!\begin{array}{|c|c|c|}\hline j & j' & n \\ \hline - & - & + \\ \hline + & & - \\ \hline & + & - \\ \hline \end{array} \quad \text{if } j' > j, \text{ or} \quad \begin{array}{c} \\ i' \\ i \\ i'' \end{array}\!\!\begin{array}{|c|c|c|}\hline j' & j & n \\ \hline - & - & + \\ \hline & + & - \\ \hline + & & - \\ \hline \end{array} \quad \text{if } j' < j.$$

In both cases, at (i, j') position we have a *wrong* + (by Lemma (4), when the square in positions (i', j), (i', j'), (i, j), (i, j') is considered), and the patterns in columns j' and n is

$$\begin{array}{c} \\ i' \\ i \\ i'' \end{array}\begin{array}{c} \begin{array}{cc} j' & n \end{array} \\ \begin{array}{|c|c|}\hline - & + \\ \hline + & - \\ \hline + & - \\ \hline \end{array} \end{array}$$

in both cases. Moreover, $\mathcal{L}'$ contains $\mathrm{V}(i', i''; j')$. However, this is impossible, since the pattern shows that at (i, j') we have a *wrong* + which is closer to the *wrong* − at (i', j') than the *wrong* + at (i'', j'): this means that when the algorithm has been applied at an early stage to produce the moves in $\mathcal{L}'$ dealing with the j'-th column, we should have contradicted the prescription according to which every vertical move contains the + which appears at the closest position to the − in that move. □

An example can be useful to understand the algorithm. Let $C(\boldsymbol{\varepsilon})$ be the configuration in dimension 7 which is generated by signs $\boldsymbol{\varepsilon} = (+, -, +, +, -, +, +)$. Thus,

$$C(\boldsymbol{\varepsilon}) = \begin{array}{|c|c|c|c|c|c|c|}\hline + & - & - & - & + & + & + \\ \hline & - & - & - & + & + & + \\ \cline{2-7} & & + & + & - & - & \\ \cline{3-7} & & & + & - & - & - \\ \cline{4-7} & & & & - & - & - \\ \cline{5-7} & & & & & + & + \\ \cline{6-7} & & & & & & + \\ \cline{7-7} \end{array}.$$

Then, applying the algorithm iteratively, we get:

$$\begin{array}{|c|}\hline + \\ \hline \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(1)} = \{\mathrm{P}(1;1)\}$$

$$\begin{array}{|c|c|}\hline + & - \\ \hline & - \\ \cline{2-2} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(2)} = \{\mathrm{H}(1;1,2)\}$$

$$\begin{array}{|c|c|c|}\hline + & - & - \\ \hline - & - & + \\ \cline{2-3} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(3)} = \{\mathrm{H}(1;1,2), \mathrm{V}(2,3;3)\}$$

$$\begin{array}{|c|c|c|c|}\hline + & - & - & - \\ \hline - & - & - & + \\ \cline{2-4} & & + & + \\ \cline{3-4} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(4)} = \{\mathrm{H}(1;1,2), \mathrm{V}(2,3;3), \mathrm{V}(1,4;4)\}$$

$$\begin{array}{|c|c|c|c|}\hline + & - & - & - \\ \hline - & - & - & + \\ \cline{2-4} & + & + & - \\ \cline{3-4} & & + & - \\ \cline{4-4} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(5)} = \{\mathrm{H}(1;1,2), \mathrm{V}(2,3;3), \mathrm{S}(1,4;4,5)\}$$

$$\begin{array}{|c|c|c|c|c|}\hline + & - & - & - & + \\ \hline - & - & - & + & + \\ \cline{2-5} & + & + & - & - \\ \cline{3-5} & & + & - & - \\ \cline{4-5} & & & - & - \\ \cline{5-5} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(6)} = \{\mathrm{H}(1;1,2), \mathrm{S}(2,3;3,6), \mathrm{S}(1,4;4,5), \mathrm{V}(5,6;6)\}$$

$$\begin{array}{|c|c|c|c|c|c|}\hline + & - & - & - & + & + \\ \hline - & - & - & + & + & + \\ \cline{2-6} & + & + & - & - & \\ \cline{3-6} & & + & - & - & - \\ \cline{4-6} & & & - & - & - \\ \cline{5-6} & & & & + & + \\ \cline{6-6} \end{array} \quad \Longrightarrow \quad \mathcal{L}^{(7)} = \left\{ \begin{array}{l} \mathrm{H}(1;1,2), \mathrm{S}(2,3;3,6), \mathrm{S}(1,4;4,5), \\ \mathrm{V}(5,6;6), \mathrm{V}(4,7;7), \mathrm{P}(1;7) \end{array} \right\}$$

References

[1] S. Astudillo, F. Diaz y Diaz, and E. Friedman. Sharp lower bounds for regulators of small-degree number fields. *J. Number Theory*, 167:232–258, 2016.

[2] M. J. Bertin. Sur une conjecture de Pohst. *Acta Arith.*, 74(4):347–349, 1996.

[3] M. Pohst. Regulatorabschätzungen für total reelle algebraische Zahlkörper. *J. Number Theory*, 9(4):459–492, 1977.

[4] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1997. Revised reprint of the 1989 original.

[5] R. Remak. Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers. *Compositio Math.*, 10:245–285, 1952.

Laboratoire de mathématiques de Besançon, Université Bourgogne Franche-Comté, CNRS - UMR 6623, 16, Route de Gray, 25030 Besançon, France
Email address: francesco.battistoni@univ-fcomte.fr

Dipartimento di Matematica, Università di Milano, via Saldini 50, 20133 Milano, Italy
Email address: giuseppe.molteni1@unimi.it