An algebraic result on the topological closure of the set of rational points on a sphere whose center is non-rational

By Jun-ichi MATSUSHITA*)

Aoyama T/G Seminar, ARIA3F 4-9-18, Jingumae, Shibuya-ku, Tokyo 150-0001
(Communicated by Heisuke HIRONAKA, M. J. A., Sept. 13, 2004)

Abstract: Let S be a sphere in $\mathbf{R}^n$ whose center is not in $\mathbf{Q}^n$. We pose the following problem on S.

"What is the closure of $S \cap \mathbf{Q}^n$ with respect to the Euclidean topology?"

In this paper we give a simple solution for this problem in the special case that the center $a = (a_i) \in \mathbf{R}^n$ of S satisfies

$$\left\{ \sum_{i=1}^{n} r_i(a_i - b_i);\ r_1, \ldots, r_n \in \mathbf{Q} \right\} = K$$

for some $b = (b_i) \in S \cap \mathbf{Q}^n$ and some Galois extension K of $\mathbf{Q}$. Our solution represents the closure of $S \cap \mathbf{Q}^n$ for such S in terms of the Galois group of K over $\mathbf{Q}$.

Key words: Sphere; rational point; topological closure; Galois group.

1. Introduction.

Notation 1. Let $\mathbf{Q}$ and $\mathbf{R}$ denote the field of rational numbers and the field of real numbers, respectively. Let $|x|$ and $\langle x,\ y \rangle$ represent the standard Euclidean norm of $x \in \mathbf{R}^n$ and the standard Euclidean inner product of $x, y \in \mathbf{R}^n$, respectively. Let $\mathrm{Cl}\, X$ represent the closure of a subset X of $\mathbf{R}^n$ with respect to the Euclidean topology, $\dim_{\mathbf{Q}(\text{resp. } \mathbf{R})} Y$ the dimension of an affine or vector space Y over $\mathbf{Q}$ (resp. $\mathbf{R}$), and $\rho(Z)$ the rank of a matrix Z. Define the symbol $\mathrm{span}_{\mathbf{Q}}$ as follows: For $z_1, \ldots, z_n \in \mathbf{R}$,

$$\mathrm{span}_{\mathbf{Q}} \{z_1, \ldots, z_n\} = \left\{ \sum_{i=1}^{n} r_i z_i;\ r_1, \ldots, r_n \in \mathbf{Q} \right\}.$$

Fix $b = (b_i) \in \mathbf{Q}^n$ and, for each $a = (a_i) \in \mathbf{R}^n$, let S_a denote the sphere through b whose center is a, that is,

$$S_a = \{x \in \mathbf{R}^n;\ |x - a| = |b - a|\}. \tag{1}$$

(Note that $b \in S_a \cap \mathbf{Q}^n$ and hence $S_a \cap \mathbf{Q}^n \neq \emptyset$.) We now pose the following problem on S_a.

Problem 2. What is $\mathrm{Cl}(S_a \cap \mathbf{Q}^n)$?

While it is not difficult to see the solution of this problem in the case $a \in \mathbf{Q}^n$ is

$$\mathrm{Cl}(S_a \cap \mathbf{Q}^n) = S_a, \tag{2}$$

it seems difficult to give some simple solution for this problem in the case $a \notin \mathbf{Q}^n$. Nevertheless, even if $a \notin \mathbf{Q}^n$, we can give a quite simple solution for this problem provided $a = (a_i)$ satisfies a special algebraic condition. The purpose of this paper is to show this fact. Let K be a Galois extension of $\mathbf{Q}$ such that $K \subset \mathbf{R}$ and $[K : \mathbf{Q}] \leq n$. Let G denote the Galois group of K over $\mathbf{Q}$ and define

$$g(a) = (g(a_i))$$

for $g \in G$, $a = (a_i) \in K^n$. Then our result is stated as follows:

Theorem 3. *If* $a = (a_i)$ *satisfies*

$$\mathrm{span}_{\mathbf{Q}} \{a_1 - b_1, \ldots, a_n - b_n\} = K, \tag{3}$$

then

$$\mathrm{Cl}(S_a \cap \mathbf{Q}^n) = \bigcap_{g \in G} S_{g(a)}. \tag{4}$$

Note that if $K = \mathbf{Q}$, then (3) and (4) coincide with $a \in \mathbf{Q}^n - \{b\}$ and (2), respectively. We prove this theorem in the following sections.

2000 Mathematics Subject Classification. Primary 14G05, 14P25; Secondary 12F10.

*) Contact Address: 6-5-15, Higashiogu, Arakawa-ku, Tokyo 116-0012.

2. Reduction of (4). For each $a \in \mathbf{R}^n$, define a hyperplane Π_a by

$$\Pi_a = \{A \in \mathbf{R}^n;\ \langle A,\ a-b\rangle + 1 = 0\}\,.$$

(Note $0 \notin \Pi_a$, that is, $\Pi_a \subset \mathbf{R}^n - \{0\}$.) The purpose of this section is to show that (4) is equivalent to

$$\text{(5)} \qquad \mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n) = \bigcap_{g\in G} \Pi_{g(a)}.$$

First we prove the following.

Proposition 4. *There is a homeomorphism (with respect to the Euclidean topology)* $\varphi : \mathbf{R}^n - \{0\} \to \mathbf{R}^n - \{b\}$ *defined by*

$$\text{(6)} \qquad \varphi(A) = b - \frac{2}{|A|^2}A.$$

Furthermore, for every $a \in \mathbf{R}^n$,

$$\text{(7)} \qquad \varphi(\Pi_a) = S_a - \{b\}$$

and

$$\text{(8)} \qquad \varphi(\Pi_a \cap \mathbf{Q}^n) = S_a \cap \mathbf{Q}^n - \{b\}$$

hold.

Proof. φ is clearly well-defined as a map. And, since each $x \in \mathbf{R}^n - \{b\}$ satisfies

$$\begin{aligned}\varphi\Big(\frac{2}{|b-x|^2}(b-x)\Big) &= b - \frac{2}{\frac{4}{|b-x|^4}|b-x|^2}\frac{2}{|b-x|^2}(b-x)\\ &= b-(b-x) = x,\end{aligned}$$

φ is surjective. We see φ is also injective, because if $\varphi(A) = \varphi(A')$, that is,

$$\text{(9)} \qquad \frac{1}{|A|^2}A = \frac{1}{|A'|^2}A',$$

then

$$\text{(10)} \qquad A' = rA$$

holds for some $r \in \mathbf{R} - \{0\}$ and, by substituting (10) to (9), we get $r = 1$, that is, $A' = A$. We have thus shown that φ is a bijection such that

$$\text{(11)} \qquad \varphi^{-1}(x) = \frac{2}{|b-x|^2}(b-x),$$

and, by the continuity of (6) and (11), we see φ is a homeomorphism. Furthermore, since

$$\begin{aligned} x \in S_a &\leftrightarrow |x-a| = |b-a|\\ &\leftrightarrow \Big\langle b-x,\ a - \frac{b+x}{2}\Big\rangle = 0\end{aligned}$$

is easily seen and $\varphi(A)$ satisfies

$$\begin{aligned}\Big\langle b-\varphi(A),\ a-\frac{b+\varphi(A)}{2}\Big\rangle &= \Big\langle \frac{2}{|A|^2}A,\ a-b+\frac{1}{|A|^2}A\Big\rangle\\ &= \frac{2}{|A|^2}(\langle A,\ a-b\rangle + 1),\end{aligned}$$

we have

$$\varphi(A) \in S_a - \{b\} \leftrightarrow \langle A,\ a-b\rangle + 1 = 0 \leftrightarrow A \in \Pi_a$$

and hence (7). By (7) and

$$A \in \mathbf{Q}^n \leftrightarrow \varphi(A) \in \mathbf{Q}^n,$$

which follows from (6) and (11), we see (8) also holds. This completes the proof. □

By noting $\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n) \subset \Pi_a \subset \mathbf{R}^n - \{0\}$ and using the fact that φ is a homeomorphism and (8), we have

$$\begin{aligned}\varphi(\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n)) &= \mathrm{Cl}(\varphi(\Pi_a \cap \mathbf{Q}^n)) - \{b\}\\ &= \mathrm{Cl}(S_a \cap \mathbf{Q}^n - \{b\}) - \{b\}\,.\end{aligned}$$

Here $\mathrm{Cl}(S_a \cap \mathbf{Q}^n - \{b\}) - \{b\}$ can be rewritten as $\mathrm{Cl}(S_a \cap \mathbf{Q}^n) - \{b\}$, because if b is an accumulation point of $S_a \cap \mathbf{Q}^n - \{b\}$, then $\mathrm{Cl}(S_a \cap \mathbf{Q}^n - \{b\}) = \mathrm{Cl}(S_a \cap \mathbf{Q}^n)$, and if b is not, then $\mathrm{Cl}(S_a \cap \mathbf{Q}^n - \{b\}) = \mathrm{Cl}(S_a \cap \mathbf{Q}^n) - \{b\}$. Hence

$$\text{(12)} \qquad \varphi(\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n)) = \mathrm{Cl}(S_a \cap \mathbf{Q}^n) - \{b\}\,.$$

On the other hand, by using the fact that φ is bijective and (7), we have

(13)

$$\varphi\Big(\bigcap_{g\in G}\Pi_{g(a)}\Big) = \bigcap_{g\in G}\varphi(\Pi_{g(a)}) = \bigcap_{g\in G} S_{g(a)} - \{b\}\,.$$

By (12), (13), and the fact that φ is bijective, we see

$$\begin{aligned}(4) &\leftrightarrow \mathrm{Cl}(S_a \cap \mathbf{Q}^n) - \{b\} = \bigcap_{g\in G} S_{g(a)} - \{b\}\\ &\leftrightarrow \varphi(\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n)) = \varphi\Big(\bigcap_{g\in G}\Pi_{g(a)}\Big)\\ &\leftrightarrow (5).\end{aligned}$$

We have thus attained the purpose of this section.

3. Proof of (5). In this section we complete the proof of Theorem 3 by proving (5) under the assumption (3). For this purpose we need the following lemma, which immediately follows from Dedekind's theorem (Bourbaki [1], Chapter V, §6, Corollary 2 of Theorem 1).

Lemma 5. *All elements of G are linearly independent over* $\mathbf{R}$.

The following is our proof of (5).

Proof. For every $g \in G$, every $A = (A_i) \in \Pi_a \cap \mathbf{Q}^n$ satisfies

$$\begin{aligned}\langle A,\ g(a) - b\rangle + 1 &= \sum_{i=1}^{n} A_i(g(a_i) - b_i) + 1 \\ &= \sum_{i=1}^{n} g(A_i)(g(a_i) - g(b_i)) + g(1) \\ &= g\biggl(\sum_{i=1}^{n} A_i(a_i - b_i) + 1\biggr) \\ &= g(\langle A,\ a - b\rangle + 1) \\ &= g(0) = 0\end{aligned}$$

and therefore, by continuity, every $A \in \mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n)$ satisfies $\langle A,\ g(a) - b\rangle + 1 = 0$. Hence we have

$$\forall g \in G \quad \mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n) \subset \Pi_{g(a)},$$

that is,

$$\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n) \subset \bigcap_{g \in G} \Pi_{g(a)}. \tag{14}$$

Hereafter let l denote $[K : \mathbf{Q}]$. We now prove

(15) $\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n)$ is a $(n - l)$-dimensional affine subspace of $\mathbf{R}^n$

as follows: As is easily seen,

$$\Pi_a \cap \mathbf{Q}^n = \biggl\{(A_i) \in \mathbf{Q}^n;\ \sum_{i=1}^{n} A_i(a_i - b_i) + 1 = 0\biggr\}$$

is an affine subspace of $\mathbf{Q}^n$. And, by

$$\mathrm{span}_{\mathbf{Q}}\,\{a_1 - b_1, \dots, a_n - b_n\} = K \ni -1,$$

this affine subspace is non-empty. Let us compute its dimension. Regard K as a l-dimensional vector space over $\mathbf{Q}$ and fix a basis of K. For each $i = 1, \dots, n$, let $(a'_{i1}, \dots, a'_{il})$ denote the coordinate of $a_i - b_i \in K$ with respect to this basis, and define

$$M = \begin{pmatrix} a'_{11} & \cdots & a'_{n1} \\ \vdots & & \vdots \\ a'_{1l} & \cdots & a'_{nl} \end{pmatrix}.$$

Then we have

$$\begin{aligned}&\dim_{\mathbf{Q}} \Pi_a \cap \mathbf{Q}^n \\ &= \dim_{\mathbf{Q}}\biggl\{(A_i) \in \mathbf{Q}^n;\ \sum_{i=1}^{n} A_i(a_i - b_i) + 1 = 0\biggr\} \\ &= \dim_{\mathbf{Q}}\biggl\{(A_i) \in \mathbf{Q}^n;\ \sum_{i=1}^{n} A_i(a_i - b_i) = 0\biggr\} \\ &= \dim_{\mathbf{Q}}\biggl\{(A_i) \in \mathbf{Q}^n;\ \forall j \in \{1, \dots, l\}\ \sum_{i=1}^{n} A_i a'_{ij} = 0\biggr\} \\ &= n - \rho(M).\end{aligned}$$

On the other hand, since the definition of M implies that $\rho(M)$ equals the dimension (over $\mathbf{Q}$) of $\mathrm{span}_{\mathbf{Q}}\,\{a_1 - b_1, \dots, a_n - b_n\} = K$, we have $\rho(M) = l$. Hence

$$\dim_{\mathbf{Q}} \Pi_a \cap \mathbf{Q}^n = n - l.$$

By this,

$$\Pi_a \cap \mathbf{Q}^n = \beta_0 + (\mathbf{Q}\beta_1 \oplus \cdots \oplus \mathbf{Q}\beta_{n-l})$$

holds for some $\beta_0, \beta_1, \dots, \beta_{n-l} \in \mathbf{Q}^n$. And it is easy to see that such $\beta_0, \beta_1, \dots, \beta_{n-l}$ satisfy

$$\mathrm{Cl}(\Pi_a \cap \mathbf{Q}^n) = \beta_0 + (\mathbf{R}\beta_1 \oplus \cdots \oplus \mathbf{R}\beta_{n-l}).$$

Thus we see (15) holds.

Next we prove

(16) $\bigcap_{g \in G} \Pi_{g(a)}$ also is a $(n - l)$-dimensional affine subspace of $\mathbf{R}^n$

as follows: Clearly $\bigcap_{g \in G} \Pi_{g(a)}$ is an affine subspace of $\mathbf{R}^n$. And, since, as we have already seen, $\Pi_a \cap \mathbf{Q}^n$ is non-empty, it follows from (14) that this affine subspace is non-empty. Let us compute its dimension. By $[K : \mathbf{Q}] = l$, G consists of exactly l elements. Let $g_1, \dots, g_l$ denote these l elements of G and define

$$N = \begin{pmatrix} g_1(a - b) \\ \vdots \\ g_l(a - b) \end{pmatrix} = \begin{pmatrix} g_1(a_1 - b_1) & \cdots & g_1(a_n - b_n) \\ \vdots & & \vdots \\ g_l(a_1 - b_1) & \cdots & g_l(a_n - b_n) \end{pmatrix}.$$

Then we have

$$\begin{aligned}&\dim_{\mathbf{R}} \bigcap_{g \in G} \Pi_{g(a)} \\ &= \dim_{\mathbf{R}}\biggl\{(A_i) \in \mathbf{R}^n;\ \forall j \in \{1, \dots, l\} \\ &\qquad \sum_{i=1}^{n} A_i(g_j(a_i) - b_i) + 1 = 0\biggr\} \\ &= \dim_{\mathbf{R}}\biggl\{(A_i) \in \mathbf{R}^n;\ \forall j \in \{1, \dots, l\} \\ &\qquad \sum_{i=1}^{n} A_i g_j(a_i - b_i) + 1 = 0\biggr\}\end{aligned}$$

$$= \dim_{\mathbf{R}} \Big\{ (A_i) \in \mathbf{R}^n;\ \forall j \in \{1, \ldots, l\} \quad \sum_{i=1}^{n} A_i g_j (a_i - b_i) = 0 \Big\}$$
$$= n - \rho(N).$$

On the other hand, we see $g_1(a-b), \ldots, g_l(a-b)$ are linearly independent over $\mathbf{R}$ and hence $\rho(N) = l$, because if $C_1, \ldots, C_l \in \mathbf{R}$ satisfy $\sum_{j=1}^{l} C_j g_j (a-b) = 0$, that is,

$$\forall i \in \{1, \ldots, n\} \quad \sum_{j=1}^{l} C_j g_j (a_i - b_i) = 0,$$

then, by the $\mathbf{Q}$-linearity of the operator $\sum_{j=1}^{l} C_j g_j : K \to \mathbf{R}$, we have

$$\forall \alpha \in \operatorname{span}_{\mathbf{Q}} \{a_1 - b_1, \ldots, a_n - b_n\} = K \quad \sum_{j=1}^{l} C_j g_j (\alpha) = 0,$$

that is, $\sum_{j=1}^{l} C_j g_j = 0$, and hence, by Lemma 5, $C_1 = \cdots = C_l = 0$. Therefore we see

$$\dim_{\mathbf{R}} \bigcap_{g \in G} \Pi_{g(a)} = n - l$$

holds and have thus proved (16).

From (14), (15), and (16), we obtain (5). This completes the proof. □

Remark 6. As is easily seen from the arguments in Section 2 and Section 3, Theorem 3 holds even if we adopt a subfield k of $\mathbf{R}$ instead of $\mathbf{Q}$ and let b, K, and G be a fixed element of k^n, a Galois extension of k such that $K \subset \mathbf{R}$, $[K : k] \leq n$, and the Galois group of K over k, respectively.

Remark 7. Let q be a non-degenerate and positive-definite quadratic form on $\mathbf{R}^n$ with coefficients in $\mathbf{Q}$ and define S_a by

$$S_a = \{x \in \mathbf{R}^n;\ q(x-a) = q(b-a)\}$$

instead of (1). Even in this case, by modifying our arguments in Section 2 slightly, we can prove that (4) is equivalent to (5) without any change of the definition of Π_a, and hence we see Theorem 3 holds.

References

[1] Bourbaki, N.: Elements of Mathematics. Algebra. Chapters 4-7. Springer, Berlin-Heidelberg-New York (1990). (Originally published as Algèbre. Chapitres 4 à 7. Lecture Notes in Mathematics, 864, Masson, Paris (1981).)