MATH. SCAND. 38 (1976), 177–191

THE PYTHAGOREAN CLOSURE OF FIELDS

MALCOLM P. GRIFFIN

0. Introduction.

A field is called Pythagorean if any sum of squares is a square. Since the intersection of any two Pythagorean fields is Pythagorean, there is a minimal Pythagorean field containing any field K; this is called the Pythagorean closure and denoted K_p.

Since any field of characteristic two is Pythagorean, because $\sum a_i^2 = (\sum a_i)^2$, we assume that all fields (except residue class fields) have characteristic not two. We use $\bar{K}$ to denote the algebraic closure of K, K^* to denote the multiplicative group of K, and $\sum K^2$ to denote the sums of squares of elements in K. Where necessary we are working inside a fixed algebraic closure. KH denotes the compositum of the field K and H in $\bar{K}$. G_K denotes the galois group of $\bar{K}$ over K. $\mathrm{Cd}_2(G)$ denotes the cohomological two dimension of G; for definitions of cohomological dimension, pro-finite groups, and for the related theorems on Galois cohomology the reader is referred to Ribes [5]; some of the results are in Serre [8].

If σ is a K-automorphism of $\bar{K}$ then $\sigma(K_p)$ is Pythagorean, so $K_p \subseteq \sigma(K_p)$, and K_p is a galois extension; the corresponding galois group is called the *pythagorean group*, denoted $\mathrm{PG}(K)$. The purpose of this paper is to investigate this group.

In the first section dealing with arbitrary fields, we show that $\mathbf{Z}_2$, the infinite pro-cyclic-2-group, which is isomorphic to the 2-adic integers, is a quotient group of $\mathrm{PG}(K)$ provided $K \neq K_p$. The second section deals with fields which are complete with respect to rank one valuations, and the third with global fields.

I am indebted to Paulo Ribenboim who thought of investigating this topic and made helpful suggestions.

1. General results.

LEMMA 1. *If K is not formally real then K_p is the quadratic closure of K.*

PROOF. It is clear that K_p is always contained in the quadratic closure.

Received October 22, 1974.

Let $-1=\sum a_i^2$. If $x \in K_p$, then

$$x = (\tfrac{1}{2}+x)^2+\sum (a_i/2)^2+\sum (a_ix)^2 \in \sum K_p{}^2 ,$$

so $\sqrt{x} \in K_p$.

$\mathrm{Py}(K)$ may be constructed as follows: Let $K_0=K$; define K_{n+1} by adjoining $\sqrt{a}$ for all $a \in \sum K_n{}^2$. Then $K_p=\bigcup_n K_n$.

LEMMA 2. *For all* n, K_n *is a Galois extension of* K.

PROOF. By induction. The statement is clearly true for $n=0$. Assume it holds for n. Let σ be a K-isomorphism of K_{n+1} into the algebraic closure of K. By induction $\sigma K_n \subseteqq K_n$. If $a_i \in K_n$, then

$$(\sigma(\sum a_i{}^2)^{\frac{1}{2}})^2 = \sigma(\sum a_i{}^2) = \sum \sigma(a_i)^2 \in \sum (K_n)^2 ,$$

so that

$$\sigma((\sum a_i{}^2)^{\frac{1}{2}}) = \pm(\sum \sigma(a_i)^2)^{\frac{1}{2}} \in K_{n+1} .$$

Let $G_n=\mathrm{Gal}(K_n|K)$, so $\mathrm{PG}(K)=\varprojlim G_n$.

LEMMA 3. $\mathrm{Gal}(K_{n+1}|K_n) \cong$ *Direct product of copies of* $\mathsf{Z}/2$.

PROOF. Since the product of any two sums of squares is again a sum of squares, and $a/b=a \cdot b/b^2$, it follows that those elements of $K_n{}^*$ which are sums of squares form a group. The corresponding subgroup of $K_n{}^*/(K_n{}^*)^2$ is a vector space over F_2, and has a basis. Let representatives of this basis in $K_n{}^*$ be $\{b_i \mid i \in I\}$. If a is a sum of squares in $K_n{}^*$, then

$$a = c^2b_1 \ldots b_t \quad \text{and} \quad \sqrt{a} \in K_n(\sqrt{b_1},\ldots,\sqrt{b_t});$$

thus $K_{n+1}=K(\bigcup_{i\in I}\sqrt{b_i})$. We prove that $\mathrm{Gal}(K_{n+1}|K_n) \cong \prod_{i\in I}\mathsf{Z}/2$. This isomorphism is given as follows: $\sigma \in \mathrm{Gal}(K_{n+1}|K_n)$ corresponds to $(\sigma_i) \in \prod_{i \in I}\mathsf{Z}/2$ where $\sigma_i=0$ if $\sigma(\sqrt{b_i})=\sqrt{b_i}$ and $\sigma_i=1$ if $\sigma(\sqrt{b_i})=-\sqrt{b_i}$.

LEMMA 4. *The maximum order of an element in* G_n *is* 2^n.

PROOF. The proof is by induction. The case $n=1$ is lemma 3. Use the exact sequence

$$1 \to \mathrm{Gal}(K_nK_{n-1}) \to G_n \xrightarrow{\varphi} G_{n-1} \to 1 .$$

Let $\sigma \in G_n$; then by induction hypothesis $[\varphi(\sigma)]^{2^{n-1}}=1$, so $\varphi(\sigma^{2^{n-1}})=1$ and $\sigma^{2^{n-1}} \in \mathrm{Gal}(K_n|K_{n-1})$, so $\sigma^{2^n}=1$.

The object of this section is to show that if $K_p \neq K$ then $\mathrm{Gal}(K_p | K)$ has Z_2 as a quotient group. We first investigate prime fields since if L is the prime field of K, then $L_p \subseteqq K_p$.

PROPOSITION 5. *Let K be an algebraic extension of F_q where q is an odd prime. Let $H = \bigcup_n F_{q^{2^n}}$. Then $K_p = K \cdot H$, and if $K_p \neq K$ then* $\mathrm{PG}(K) = \mathsf{Z}_2$.

PROOF. By lemma 1, K_p is the quadratic closure of K. Let $x \in K_p$; then $x \in F_t(x)$ where $F_t \subseteqq K$ and $[F_t(x) : F_t] = 2^n$. Thus the order of $F_t(x)$ is t^{2^n} and $F_t(x) \subseteqq F_t \cdot H$, so that $K_p \subseteqq KH$. Since every element in a field of characteristic not two has two distinct roots and only half the elements in finite fields of odd characteristic have square roots, $(F_q)_p$ must be infinite. Since $(F_q)_p \subseteqq H$ it follows that $(F_q)_p = H$. Thus

$$\mathrm{Gal}(F_q)_p | F_q) = \varprojlim \mathrm{Gal}(F_{p^{2^n}} | F_p) = \mathsf{Z}_2 .$$

H is the field obtained by adjoining the 2^n roots of unity to F_p for all n. Since $H \subseteqq K_p \subseteqq KH$, $K_p = KH$ and $\mathrm{Gal}(K_p | K) = \mathrm{Gal}(L | K \cap L)$ is either Z_2 or zero.

PROPOSITION 6. *Let ξ_n be a primitive 2^{n+2} root of unity, $h_n = \xi_n + \xi_n^{-1}$, $H_n = \mathsf{Q}(h_n)$ and $H = \bigcup_n H_n$. Then $H \subseteqq \mathsf{Q}_p$ and* $\mathrm{Gal}(H | \mathsf{Q}) = \mathsf{Z}_2$.

PROOF. Let R be any real closure of Q. Let σ be the R automorphism of $\overline{\mathsf{Q}}$. Since $\sigma(\xi_n) = \xi_n^{-1}$, $H_n \subseteqq R$. ξ_n satisfies $X^2 - h_n X + 1 = 0$, so that $\mathsf{Q}(\xi_n)$ is a quadratic extension of H_n. It is well known that

$$\mathrm{Gal}(\mathsf{Q}(\xi_n) | \mathsf{Q}) = \mathsf{Z}/2^n \times \mathsf{Z}/2 .$$

Since $\sqrt{-1} \notin H_n$, H_n contains only one quadratic extension of Q and

$$\mathrm{Gal}(H_n | \mathsf{Q}) = \mathsf{Z}/2^n .$$

H_n is obtained from Q by a sequence of quadratic extensions; since every ordering of Q extends to H_n each of these quadratic extensions must be obtained by adjoining the square root of an element which is positive in all orderings, and thus is a sum of squares. Thus $H_n \subseteqq \mathsf{Q}_p$ and consequently $H \subseteqq \mathsf{Q}_p$. Finally

$$\mathrm{Gal}(H | Q) = \varprojlim \mathrm{Gal}(H_n | \mathsf{Q}) = \varprojlim \mathsf{Z}/2^n = \mathsf{Z}_2 .$$

We continue to use H to denote the extensions of the prime field defined in the two previous propositions.

COROLLARY 7. *Let K be any field. Either* $\mathrm{Gal}(KH\,|\,K)=\mathsf{Z}_2$ *or* $K\supseteqq H$. *In the first case* Z_2 *is a quotient group of* $\mathrm{PG}(K)$; *the second case occurs if and only if* $K(i)$ *contains the* 2^n*-th roots of unity for all* n.

PROOF. Since $H\subseteqq K_p$, $\mathrm{Gal}(KH\,|\,K)=\mathrm{Gal}(H\,|\,K\cap H)$ is a quotient group of $\mathrm{PG}(K)$. But if $\mathrm{Gal}(H\,|\,K\cap H)$ is not Z_2 it must be trivial so that $H\subseteqq K$.

Since H already contains the 2^nth roots of unity unless K has characteristic zero, we need only prove that if K has characteristic zero, $K(i)\supseteqq H(i)$ implies that $K\supseteqq H$. Suppose $K\not\supseteqq H(i)$.

$$\mathrm{Gal}(K(i)\,|\,K) = \mathrm{Gal}(H(i)K\,|\,K) = \mathrm{Gal}(H(i)\,|\,K\cap H(i)) .$$

Since $[K(i):K]\leqq 2$, $[H(i):K\cap H(i)]\leqq 2$, so $H(i)\cap K$ is a subfield of $H(i)$ having index two. Since

$$\mathrm{Gal}(H(i)\,|\,\mathsf{Q}) = \mathsf{Z}_2\times \mathsf{Z}/2$$

there is only one subfield of index two in $H(i)$; it must be H.

Let $c=1+a^2$ be any element in K but not in K^2. Define f_n inductively as follows:

$$f_1 = c^{-\frac{1}{2}}, \quad f_{n+1} = 2^{-\frac{1}{2}}(1+f_n)^{\frac{1}{2}} .$$

Let

$$f'_{n+1} = 2^{-\frac{1}{2}}(1-f_n)^{\frac{1}{2}} \quad \text{for } n\geqq 1$$

and $f_1'=ac^{-\frac{1}{2}}$. Let $g_n=f_n+if_n'$.

LEMMA 8. $f_n\in K_n$.

PROOF. We prove by induction that $f_n\in K_n$ and $1-f_n^2\in\sum(K_{n-1})^2$. Denote K by K_0. Clearly $f_1\in K_1$, and

$$1-f_1^2 = 1-1/c = a^2/c\in\sum K^2 .$$

Assume the statement holds for n.

$$(f_{n+1})^2 = \tfrac{1}{2}(1+f_n) = \tfrac{1}{4}(1+f_n)^2+\tfrac{1}{4}(1-f_n^2)\in K_n^2+\sum(K_{n-1})^2\subseteqq\sum K_n^2;$$

thus $f_{n+1}\in K_{n+1}$.

$$1-(f_{n+1})^2 = 1-\tfrac{1}{2}(1+f_n) = \tfrac{1}{4}(1-f_n)^2+\tfrac{1}{4}(1-f_n^2)\in K_n^2+\sum(K_{n-1})^2\subseteqq \sum K_n^2 .$$

LEMMA 9. ${g_m}^{2^m}$ *is in the same square class over* $K(i)$ *as* c.

PROOF. We first show that if $n \geqq 1$, then $f_{n+1}f'_{n+1} = \frac{1}{2}f_n'$ and $(g_{n+1})^2 = g_n$. If $n > 1$,

$$f_{n+1}f'_{n+1} = \tfrac{1}{2}(1-f_n)^{\frac{1}{2}}(1+f_n)^{\frac{1}{2}} = \tfrac{1}{2}(1-f_n{}^2)^{\frac{1}{2}} = \tfrac{1}{2}(1-\tfrac{1}{2}(1+f_{n-1}))^{\frac{1}{2}}$$
$$= \tfrac{1}{2}2^{-\frac{1}{2}}(1-f_{n-1})^{\frac{1}{2}} = \tfrac{1}{2}f_n' ,$$

and

$$f_2f_2' = \tfrac{1}{2}(1-f_1{}^2)^{\frac{1}{2}} = \tfrac{1}{2}(1-1/c)^{\frac{1}{2}} = \tfrac{1}{2}ac^{-\frac{1}{2}} = \tfrac{1}{2}f_1' .$$

Thus if $n \geqq 1$

$$(g_{n+1})^2 = (f_{n+1}+if'_{n+1})^2 = (f_{n+1})^2-(f'_{n+1})^2+2if_{n+1}f'_{n+1}$$
$$= \tfrac{1}{2}(1+f_n-(1-f_n))+2i\tfrac{1}{2}f_n' = f_n+if_n' = g_n .$$

The lemma is now clear for $g_m{}^{2^m} = g_1{}^2 = c^{-1}(1+ia)^2$ which is in the same square class as c.

REMARK. Since $f'_{n+1} = \frac{1}{2}f_n'/f_{n+1}$ for $n \geqq 1$ and $f_1' = af_1$, it follows by induction that $K(f_n') = K(f_n)$ and hence that $K(g_n) = K(f_n)(i)$.

THEOREM 10. *If K is not pythagorean then there exists a galois extension L of K contained in K_p such that* $\mathrm{Gal}(L|K) = \mathbf{Z}_2$.

PROOF. If $K \not\supseteq H$ the theorem follows from corollary 7. If K contains the 2^nth roots of unity for all n and $K \neq K_p$, then K has a quadratic extension $K(\sqrt{a})$, and it follows by Kummer theory that if $L = \bigcup_n K(a^{2^{-n}})$, then $\mathrm{Gal}(L|K) = \mathbf{Z}_2$. Thus the only case of interest is $K \neq K_p$, $K \supseteq H$ and $K \neq K(i)$.

If K is not formally real then there is a minimum value of n such that $1+a_1{}^2+\ldots+a_n{}^2 = 0$. Since $i \notin K$, $n \geqq 2$, and as is well known, $n+1$, the level of the field, must be a power of two, so $n \geqq 3$. Thus if $c = 1+a_1{}^2$, c is not in the same square class as -1. By the previous lemma, $K(g_n)$ is a cyclic extension of $K(i)$ of degree 2^n and $[K(g_n):K] = 2^{n+1}$. If K is formally real, choose $c = 1+a^2 \notin K^2$; then $[K(g_n):K] = 2^{n+1}$ and $K(g_n)$ is a cyclic extension of $K(i)$.

We shall prove that $K(f_n)$ is a cyclic extension of K having degree 2^n. The result then follows by setting $L = \bigcup_n K(f_n)$.

Let σ be the generating automorphism of $K(f_n)(i)|K(f_n)$. Since $f_n' \in K(f_n)$,

$$\sigma(f_n+if_n') = f_n-if_n' .$$

If $n > 1$,

$$g_n\sigma(g_n) = (f_n+if_n')(f_n-if_n') = f_n{}^2+(f_n')^2$$
$$= \tfrac{1}{2}(1+f_{n-1})+\tfrac{1}{2}(1-f_{n-1}) = 1;$$
$$g_1\sigma(g_1) = f_1{}^2+(f_1')^2 = 1/c+a^2/c = 1 .$$

Consequently, $\sigma(g_n) = g_n{}^{-1}$.

Let ξ be a primitive 2^nth root of unity. Since $H \subseteq K$ it follows that σ must interchange the roots of the polynomial

$$X^2 - (\xi + \xi^{-1})X + 1 = 0 ,$$

i.e. that $\sigma(\xi) = \xi^{-1}$. $\mathrm{Gal}(K(g_n) \mid K(i))$ is generated by τ where $\tau(g_n) = \xi g_n$. Consequently

$$\begin{aligned} \sigma\tau(g_n) &= \sigma(\xi g_n) = \sigma(\xi)\sigma(g_n) = \xi^{-1} g_n{}^{-1} \\ &= (\xi g_n)^{-1} = \tau(g_n)^{-1} = \tau(g_n{}^{-1}) = \tau\sigma(g_n) . \end{aligned}$$

Thus τ and σ commute. Since $K(i) \cap K(f_n) = K$, τ and σ are K-automorphisms of $K(g_n)$ and $[K(g_n):K] = 2^{n+1}$; $K(g_n)$ is a galois extension of K with group $\mathsf{Z}/_2 n \times \mathsf{Z}/2$. Thus $K(f_n)$ is cyclic of degree 2^n.

The result that $\mathrm{Gal}(K_p \mid K)$ is either trivial or has Z_2 as quotient group generalizes the result of Diller and Dress [2] that if $\mathrm{Gal}(K_p \mid K)$ is non-trivial, then $\mathsf{Z}/4$ is a quotient group. It is possible to have $\mathrm{Gal}(K_p \mid K) = \mathsf{Z}_2$. Take K a maximal subfield of $\overline{\mathsf{Q}}$ which does not contain $\sqrt{2}$. Intersect this field with some real closure of the rationals if a formally real field is desired cf. [3, exercise 3, chapter 8]. By forming fields of the type $K = k((X_1))((X_2)) \dots ((X_n))$ where k is algebraically closed, we obtain fields such that $\mathrm{PG}(K) = \prod_n \mathsf{Z}_2$, as we shall see later.

$\mathrm{PG}(K)$ contains no torsion elements, for if $\sigma^{2^n} = 1$ then the fixed field L of σ has finite index in K_p and since $L_p = K_p$, $\mathrm{PG}(L)$ is finite, so Z_2 is not a quotient group, $L = L_p = K_p$, and σ is the identity.

PROPOSITION 11. *If the fixed field L of an abelian subgroup A of* $\mathrm{PG}(K)$ *does not contain H then $LH = K_p$ and $A = \mathsf{Z}_2$.*

PROOF. We suppose that $LH \neq K_p$ and deduce that $H \subseteq L$. Let $c = 1 + a^2$ be chosen as in the preceding theorem if $\sqrt{-1} \notin L$; otherwise take c an arbitrary non square. Thus LH has a cyclic extension M of degree m generated by f_m (respectively $c^{2^{-m}}$). Since $M \mid L$ is abelian, f_m (respectively $c^{2^{-m}}$) generates a cyclic extension of L. In the case of $c^{2^{-m}}$ the automorphism is given by $c^{2^{-m}} \to \xi_m c^{2^{-m}}$ where ξ_m is a primitive 2^mth root of unity, and hence $\xi_m \in L$, so $\xi_m + \xi_m{}^{-1} \in L$. Otherwise $\tau\colon g_m \to \xi_m g_m$ is the generating automorphism over $L(i)$ so that

$$\begin{aligned} \tau(f_m) + \tau^{-1}(f_m) &= \tau(g_m + g_m{}^{-1}) + \tau^{-1}(g_m + g_m{}^{-1}) \\ &= \xi_m g_m + \xi_m{}^{-1} g_m{}^{-1} + \xi_m{}^{-1} g_m + \xi_m g_m{}^{-1} \\ &= (\xi_m + \xi_m{}^{-1})(g_m + g_m{}^{-1}) = (\xi_m + \xi_m{}^{-1}) f_m . \end{aligned}$$

Thus $\xi_m + \xi_m^{-1} \in L$. Since m is arbitrary this proves $H \subseteq L$, a contradiction. It follows that $LH = K_p$ and consequently that $A = \mathsf{Z}_2$.

PROPOSITION 12. *If* $\mathrm{Cd}_2(G_{HK}) \leqq 1$ *and* $K \neq K_p$, *then the maximal abelian closed subgroup of* $\mathrm{PG}(K)$ *is* Z_2.

PROOF. Let A be a maximal abelian closed subgroup with fixed field L. Suppose $A \neq \mathsf{Z}_2$; then $L \supseteqq KH$, so that $\mathrm{Cd}_2(G_L) \leqq 1$ by Proposition 5.1, page 271 of [5]. In particular this implies that L is not formally real. It follows by corollary 3.2, page 255 of [5] that $\mathrm{PG}(L)$ is a free pro-2-group. Since it is also abelian, and contains Z_2 it must be Z_2.

The hypothesis of this proposition holds if K is any algebraic extension of Q which is not formally real (see theorem 8.8, page 302 of [5]). The example quoted previously where $\mathrm{PG}(K) = \prod_n \mathsf{Z}_2$, shows that the maximal abelian closed subgroup may be larger than Z_2.

2. Fields complete with respect to a rank one valuation.

K is a field complete with respect to the rank one valuation v. k is the residue class field. If v is discrete, π denotes a uniformizing element. Although we exclude the case where K has characteristic two we now generalize our notation to deal with the case k has characteristic two. If k has characteristic two, define $k_0 = k$ and k_{n+1} to be the union of all separable quadratic extensions of k_n; define $k_p = \bigcup_n k_n$ and $\mathrm{PG}(k) = \mathrm{Gal}(k_p \mid k)$.

Let $K_{n,u}$ denote the maximal unramified extension of K in K_n and $K_{p,u}$ that of K in K_p

PROPOSITION 13. *Let K be complete with respect to a rank one valuation. The residue field of K_p is k_p and there is an exact sequence*

$$0 \to \mathrm{PG}(K_{p,u}) \to \mathrm{PG}(K) \to \mathrm{PG}(k) \to 0\,.$$

PROOF. If k is not formally real, -1 is a sum of squares in k and by Hensels lemma, -1 is a sum of squares in K. Thus K_p coincides with the quadratic closure of K, and k_p with the separable quadratic closure of k. The one to one correspondence between the unramified extension of K and the separable extensions of k established by going to residue class fields gives isomorphic Galois groups and establishes $\mathrm{Gal}(K_{p,u} \mid K) \cong \mathrm{PG}(k)$.

If k is formally real we need to establish that the above correspondence takes subfields of $K_{p,u}$ into subfields of k_p. It suffices to do this for quadratic extensions, since any such subfield of finite degree is obtained by a sequence of quadratic extension. Let $L=K(\sum a_i^2)^{\frac{1}{2}}$ be such an extension. Since L is unramified we may assume that $v(a_1)=0$ and that $v(a_i)\geqq 0$. The corresponding residue class field is $\bar{L}=k((\sum \bar{a}_i^2)^{\frac{1}{2}})$, where bar denotes the map to the residue class field, and clearly $\bar{L}\subseteq k_p$.

The final result now follows from the exact sequence:

$$0 \to \mathrm{PG}(K_{p,u}) \to \mathrm{PG}(K) \to \mathrm{Gal}(K_{p,u}|K) \to 0 .$$

PROPOSITION 14. *If K is complete with respect to a rank one valuation and the residue class field has characteristic two, then* $\mathrm{PG}(k)$ *is a free pro-2-group of rank* $\dim_{\mathsf{F}_2}(k|f(k))$ *where* $f: x \to x^2 - x$. *In particular, if k is finite then* $\mathrm{PG}(k)=\mathsf{Z}_2$. *If k is perfect and* $2\nmid[\bar{k}:k_p]$, *then* $\mathrm{PG}(K_{p,u})$ *is a free pro-2-group of rank* $\dim(K_p{}^*:(K_{p,u}^*)^2]$. *In particular, if k is algebraic over* F_2 *then* $\mathrm{PG}(K_{p,u})$ *is a free pro-2-group of countable rank.*

PROOF. The first result is corollary 3.4, page 257 of [5]. If k is finite, $k|f(k)$ contains two elements, so the rank is one, so $\mathrm{PG}(k)=\mathsf{Z}_2$. By theorem 6.1, page 277 of [5],

$$\mathrm{Cd}_2(G_{K_{p,u}}) = 1+\mathrm{Cd}_2(G_{k_p}) = 1 ,$$

for, since $2\nmid[\bar{k}:k_p]$, $\mathrm{Cd}_2(G_{K_p})=0$, corollary 2.3, page 208 [5]. Consequently $\mathrm{PG}(K_{p,u})$ is a free pro-2-group by corollary 3.2, page 255 of [5]. By the remark on page 262 of [5] the rank of this free group is $\dim(K_{p,u}^*|(K_{p,u}^*)^2)$. For a local field, $[K^*:(K^*)^2]=4(\sharp k)^t$ where $(\pi)^t=(2)$. Consequently $[K_{p,u}^*:(K_{p,u}^*)^2]$ is countable in this case. It is also true in this case that $2\nmid[\bar{k}:k_p]$. The result follows.

PROPOSITION 15. *Let K be complete with respect to a rank one valuation v with k not of characteristic two. Then* $\mathrm{PG}(K_{p,u})$ *is a torsion free abelian pro-2-group. If v is discrete and k is not formally real, then* $\mathrm{PG}(K_{p,u})=\mathsf{Z}_2$, *and if in addition k contains the 2^n-th roots of unity for all n then* $\mathrm{PG}(K)\cong \mathsf{Z}_2\oplus\mathrm{PG}(k)$.

PROOF. First observe that if k is formally real, then $K_p=K_{p,u}$ so that $\mathrm{PG}(K_{p,u})=0$. For suppose that

$$\alpha = \sum_{i=1}^m \alpha_i^2 \quad \text{with } \alpha_i \in K .$$

Let $v(\alpha_j)=\min_{1\leq i\leq m}\{v(\alpha_i)\}$. Then $v(\alpha)=2v(\alpha_j)$, for otherwise the map φ to the residue class field would give $0=\sum_{i=1}^m \varphi(\alpha_i/\alpha_j)$, contradicting the assumption that k is formally real.

If k is not formally real, k_p and hence $K_{p,u}$ contains the 2^nth roots of unity for all n. Thus, by theorem 3, page 64 of [6], $\mathrm{PG}(K_{p,u})$ is abelian.

If k is not formally real then neither is K and π is a sum of squares; so $\mathrm{PG}(K_{p,u})$ contains Z_2, but every tamely ramified galois extension is cyclic for a discrete valuation so $\mathrm{PG}(K_{p,u}) \cong \mathsf{Z}_2$. If k contains the 2^nth roots of unity so does K; consequently adjoining the 2^nth roots of π to K is a cyclic extension for all n. Thus K has a totally and tamely ramified extension with galois group Z_2 and consequently $\mathrm{PG}(K) = \mathsf{Z}_2 \oplus \mathrm{PG}(k)$.

PROPOSITION 16. *Let K be complete with respect to a discrete valuation having as residue class field k an algebraic extension of F_p where p is odd. If $H \subseteq k$ then $\mathrm{PG}(K) = \mathsf{Z}_2$; otherwise $k \cap H = \mathsf{F}_q$, with $q = p^{2^m}$ and $\mathrm{PG}(K) = \varprojlim G_n$ where G_n is given by generators and relations*:

$$\{\sigma, \tau \mid \sigma^{2^n} = \tau^{2^n} = \sigma^{-1}\tau^t\sigma\tau^{-1} = \mathrm{id}\}$$

and $t = 2^s \pm 1$ is the residue of $q \bmod 2^{s+1}$ where s is the largest integer such that $q = \pm 1 \pmod{2^s}$.

PROOF. If $H \subseteq k$ the proof is clear from our previous results. Thus to complete the proof we must calculate $G_n = \mathrm{Gal}(K_n | K)$. $K_n = K_{n,u}(\mu)$ where μ is a 2^nth root of π. $K_{n,u}$ corresponds to $k_n = \mathsf{F}_{q2^n}.k$. Let $d = 2^{s+n}$. Let x be a primitive dth root of unity over F_q and y be a square root of x. We show that $y \notin k_n$, $k_n = k(x)$ and $\varphi : x \to x^t$ generates the galois group of k_n over k. k_n is a field with $q^{2^n b}$ elements where b is odd. Now

$$\begin{aligned} q^{2^n b} - 1 &= (a2^s \pm 1)^{2^n b} - 1 \\ &\equiv 1 \pm 2^{n+s}ab - 1 \bmod 2^{n+s+1} \\ &\equiv 2^{n+s} \bmod 2^{n+s+1} \equiv d \bmod 2d\,. \end{aligned}$$

Consequently y raised to $q^{2^n b} - 1$ is the same as y^d which is -1. Thus $y \notin k_n$ but $y^2 = x \in k$. It follows that $k_n = k(x)$.

$$\begin{aligned} t^{2^{n-1}} &= (2^s \pm 1)^{2^{n-1}} = 1 \pm 2^{s+n-1} + c2^{2s+n-2} \\ &\equiv 1 + \tfrac{1}{2}d \bmod d\,. \end{aligned}$$

Thus $\varphi^{2^{n-1}}(x) = x^{1+d/2} = -x$ so φ has order 2^n, and thus generates the galois group.

Let ξ be a primitive dth root of unity in K which maps into x in the residue field. Then $K_{n,u} = K(\xi)$ and $\xi \to \xi^t$ generates the galois group. $\sigma : \xi \to \xi^t$ also generates the galois group of $K(\mu, \xi)$ over $K(\mu)$. Let $e = 2^s$ and $f = 2^n$. Then $\tau : \mu \to \xi^e\mu$ generates the galois group of K_n over $K_{n,\mu}$, since ξ^e is a primitive fth root of unity. $K_n = K(\xi, \mu) = K(\xi + \mu)$, for since $K(\xi+\mu)$ has the same residue class field as $K(\xi)$, $K(\xi) \subseteq K(\xi+\mu)$. σ and τ define K-automorphism of K_n by

$$\tau: \xi + \mu \to \xi + \xi^e \mu \quad \text{and} \quad \sigma: \xi + \mu \to \xi^t + \mu ,$$

and

$$\sigma^f = \tau^f = \mathrm{id} .$$

Since the fixed fields of σ and τ are respectively unramified and totally ramified, $\langle\sigma\rangle \cap \langle\tau\rangle = \mathrm{id}$, and the order of the group generated by σ and τ is $f^2 = [K_n : K]$; they generate $\mathrm{Gal}(K_n | K)$. Finally,

$$\sigma\tau(\xi+\mu) = \sigma(\xi + \xi^e\mu) = \xi^t + \xi^{et}\mu = \tau^t(\xi^t + \mu) = \tau^t\sigma(\xi+\mu) ,$$

so $\sigma\tau = \tau^t\sigma$.

COROLLARY 17. *If $t = 2^s + 1$ then the largest abelian quotient group of* $\mathrm{PG}(K)$ *is* $\mathsf{Z}_2 \times \mathsf{Z}/2^s$; *otherwise it is* $\mathsf{Z}_2 \times \mathsf{Z}/2$. *The latter case occurs if and only if* $q \equiv 3 \pmod 4$ *and in this case* $\mathrm{PG}(K)$ *has the dihederal group as a quotient group.*

A more explicit computation of the K_p is possible for discrete valuations in the equal characteristic case; here $K = k((x))$ is a power series field. We define

$$K^{(\frac{1}{2})} = \bigcup_n k((X^{2^{-n}})) .$$

PROPOSITION 18. *$K_p = k_p K'$ where $K' = K$ if k is formally real and otherwise $K' = K^{(\frac{1}{2})}$.*

PROOF. If k is not formally real then Y is a sum of squares in $k((Y))$, and Y is not a square since the square of an element in $k((Y))$ must start with a term of even degree. Thus $Y^{\frac{1}{2}}$ belongs to $k((Y))_p$, and for each $n, X^{2^{-n}} \in K_p$. Consequently $K^{(\frac{1}{2})} \subseteq k((X))_p$, provided that k is not formally real. Also $k_p \subseteq k((X))_p$ and consequently, $k_p . K' \subseteq K_p$.

We need to show that if $a, b \in k_p . K'$ then $(a^2 + b^2)^{\frac{1}{2}} \in k_p K'$. If k is not formally real then $a, b \in k_p . K^{(\frac{1}{2})}$ and there is some integer n such that $a, b \in k_p k((X^{2^{-n}}))$. Let $Y = X^{2^{-n}}$. If k is formally real, $a, b \in k_p . K$, set $Y = X$. By multiplying by a suitable power of Y we may assume that a is of the form $a_0 + a_1 Y + a_2 Y^2 + \ldots$ with $a_0 \neq 0$ and that b is of the form $b_0 + b_1 Y + b_2 Y^2 + \ldots$. Since a, b are in the compositum $k_p k((Y))$, all the a_i, b_i are in some finite extension k_1 of k with $k \subseteq k_1 \subseteq k_p$. Now

$$a^2+b^2 = a_0^2+b_0^2+2(a_0a_1+b_0b_1)Y+(a_1^2+b_1^2+2(a_0a_2+b_0b_2))Y^2+ \\ +2(a_0a_3+a_1a_2+b_0b_3+b_1b_2)Y^3+\ldots .$$

If $a_0^2+b_0^2 \neq 0$ (this will always be the case if k is formally real) then we can solve for the coefficients of a power series c with $c^2=a^2+b^2$;

$$c_0 = (a_0^2+b_0^2)^{\frac{1}{2}}, \quad c_1 = c_0^{-1}(a_0a_1+b_0b_1)$$
$$c_2 = (2c_0)^{-1}(a_1^2+b_1^2-c_1^2+2(a_0a_2+b_0b_2)) \text{ etc.}$$

and we have $c \in k_1((a_0^2+b_0^2)^{\frac{1}{2}})((Y)) \subseteq k_p.K'$. If $a_0^2+b_0^2=0$ let $d_nY^n+d_{n+1}Y^{n+1}+\ldots$ be the power series for a^2+b^2. Since k is not formally real, d_n is a sum of squares. Let $k_2=k_1(\sqrt{d_n})$. Let $Z=Y^{\frac{1}{2}}$ and let

$$c = c_nZ^n+c_{n+1}Z^{n+1}+\ldots$$

be such that $c^2=a^2+b^2$. Then

$$c_n = \sqrt{d_n}, \quad 2c_nc_{n+1} = 0, \text{ etc.}$$

and we can solve for c_n, c_{n+1}, c_{n+2}, etc. Consequently

$$c \in k_2((Z)) = k_2((X^{2^{-n-1}})) \subseteq k_2.k((X))^{\frac{1}{2}} \subseteq k_p.K' .$$

Corollary 19. *$k((X))$ is pythagorean if and only if k is pythagorean and formally real. If K is formally real then* $\mathrm{PG}(K) \cong \mathrm{PG}(k)$.

Note. In general it is not true that $k_p((X))=k_p.k((X))$. For example take $k=\mathbf{Q}$.

Power series provide a good example showing that the compositum of two pythagorean fields need not be pythagorean. Let R_1 and R_2 be two different real closures of $\mathbf{Q}$ in $\overline{\mathbf{Q}}$. Then $R_1((X))$ and $R_2((X))$ are both formally real pythagorean subfields of $\overline{\mathbf{Q}}((X))$; however their compositum is not formally real, and thus not pythagorean (for it does not contain $\sqrt{X}$).

To end this section we discuss the relationship between pythagorean closure and completion with respect to a rank one valuation. $\hat{K}$ denotes the completion of K.

Lemma 20. *Let $\hat{K}$ be the completion of K with respect to the rank one valuation v. Let $a \in \sum \hat{K}^2$; then there exists $b \in \sum K^2$ such that $\hat{K}(\sqrt{a})=\hat{K}(\sqrt{b})$.*

PROOF. Let $a=\sum_{i=1}^{n} a_i^2$. Multiplying by an even power of an element with value one we may assume $0 \leqq v(a_i)$, $1 \leqq i \leqq n$. Let $v(a)=t$. Let $b_i \in K$ be chosen such that

$$v(b_i - a_i) > 2v(2)+t, \quad 1 \leqq i \leqq n ,$$

and set $b=\sum_{i=1}^{n} b_i^2$. Now apply Hensels lemma [1, page 34] to the field $K(\sqrt{a})$.

$$X^2 - b = (X-\sqrt{a})(X+\sqrt{a}) + a - b ,$$
$$(X-\sqrt{a}) + (-1)(X+\sqrt{a}) = 2\sqrt{a} ,$$

and

$$v(a-b) = v(\sum (a_i^2 - b_i^2)) \geqq \min\{v(a_i - b_i) + v(a_i + b_i)\}$$
$$> 2v(2)+t \geqq v(2^2)+v(a) \geqq v((2\sqrt{a})^2) ,$$

so X^2-b factorizes in $\hat{K}(\sqrt{a})$. Since $v(b)=v(a)$ the same argument shows that X^2-a factorizes in $\hat{K}(\sqrt{b})$ and it follows that $\hat{K}(\sqrt{a})=\hat{K}(\sqrt{b})$.

PROPOSITION 21. *Let v be a rank one valuation of K. Identify the algebraic closure of K in that of $\hat{K}$; then $(\hat{K})_p = K_p . \hat{K}$.*

PROOF. Since $K \subseteqq (\hat{K})_p$, $K_p \subseteqq (\hat{K})_p$ and so $K_p . \hat{K} \subseteqq (\hat{K})_p$. Let $x \in (\hat{K})_p$; then $\hat{K}(x)$ may be obtained from $\hat{K}$ by a sequence of quadratic extensions in $(\hat{K})_p$,

$$\hat{K} = K_0 \subseteqq K_1 \subseteqq K_2 \ldots \subseteqq K_n = \hat{K}(x) .$$

We show there exists a sequence of fields in K_p,

$$K = L_0 \subseteqq L_1 \subseteqq \ldots \subseteqq L_n$$

such that $L_i\hat{K}=K_i$; this will show $\hat{K}(x) \subseteqq \hat{K}.K_p$. By induction we need only prove that if $L_iK=K_i$ and $K_{i+1}=K_i(\sqrt{a})$, then there exists b such that

$$b \in K_p, \quad L_i(\sqrt{b})\hat{K} = K_{i+1} .$$

Choose b according to the previous lemma using the fact that $\hat{L}_i = L_i\hat{K} = K_i$.

COROLLARY 22. *If K is pythagorean so is its completion with respect to any rank one valuation.*

It should be noted that $(K_p)^\wedge \neq (\hat{K})_p$. $K \subseteqq (K_p)^\wedge$, so $\hat{K} \subseteqq (K_p)^\wedge$ and since $(K_p)^\wedge$ is pythagorean, $(\hat{K})_p \subseteqq (K_p)^\wedge$; however the case $K=\mathbf{Q}(X)$ with the valuation given by X provides a counter example to the opposite inclusion. For if h_n is the sum of a primitive 2^nth root of unity and its inverse, then $h_n \in \mathsf{Q}(X)_p$ so that

$$h = \sum h_n X^n \in (\mathsf{Q}(X)_p)\hat{}\ .$$

However $(\mathsf{Q}(X)\hat{})_p = (\mathsf{Q}((X)))_p = \mathsf{Q}_p . \mathsf{Q}((X))$ does not contain h.

3. Global fields.

PROPOSITION 22. *If K is a global field which is not formally real, then there is an exact sequence*

$$0 \to F_c \to \mathrm{PG}(K) \to \mathsf{Z}_2 \to 0$$

where F_c is the free pro-2-group on a countable number of generators.

PROOF. First case: K is a finite algebraic extension of $\mathsf{F}_p(X)$. Since $\mathsf{F}_p H$ has no quadratic extensions, $\mathrm{cd}_2(\mathsf{F}_p H) = 0$ and by proposition 5.2, page 272 of [5], $\mathrm{cd}_2(\mathsf{F}_p H(X)) = 1$. By proposition 5.1, page 271 of [5], the same is true of any finite algebraic extension of $H(X)$, in particular of KH. Consequently $\mathrm{PG}(KH)$ is a free pro-2-group by corollary 3.2, page 255 of [5]. The rank of this free group is countable since that is the order of $H(X)^*/H(X)^{*2}$ by remark, page 262 of [5]. Finally $\mathrm{Gal}(KH \mid K) = \mathsf{Z}_2$.

Second case: K is an algebraic number field which is not formally real. $2 \mid [\bar{K} : KH]$ and at every non archimedean valuation v of KH, $2^\infty \mid [(KH)_v : \mathsf{Q}_v]$, and so by theorem 8.8, page 302 of [5], $\mathrm{cd}_2(\mathrm{PG}(KH)) = 1$, implying that $\mathrm{PG}(KH)$ is a free pro-2-group. By square classes its rank is countable. Since $\mathrm{Gal}(KH \mid K) = \mathsf{Z}_2$ the result follows.

The methods used above do not apply to the formally real case since in this case the cohomological two-dimension is always infinite. I cannot see how to treat this case.

PROPOSITION 23. *Let A be a direct product of a countable number of finite cyclic two groups, and let K be an algebraic number field; then $\mathsf{Z}_2 \oplus A$ is a quotient group of* $\mathrm{PG}(K)$.

PROOF. Let ξ_p be a primitive pth root of unity for some odd prime p. $\xi_p + \xi_p^{-1}$ generates a cyclic extension of Q of order $\frac{1}{2}(p-1)$, which is in all real closures of Q. Let $n(p)$ denote the largest power of two dividing $\frac{1}{2}(p-1)$, and let $\mu_p \in \mathsf{Q}(\xi_p + \xi_p^{-1})$ generate the cyclic extension of Q having order $2^{n(p)}$. $\mathsf{Q}(\mu_p)$ is obtained by quadratic extensions, and is in all real closures of Q, so it is contained in Q_p.

It follows from Dirichlet's theorem that there are an infinite number of primes in the arithmetic progression $2^{a+2}m+2^{a+1}+1$, and thus that there are an infinite number of primes with $n(p)=a$.

Let T_p be the field generated by $\bigcup_{q\neq p}\mathsf{Q}(\xi_q)$; then by statement (b) of chapter VIII of [4], $T_p \cap \mathsf{Q}(\xi_p)=\mathsf{Q}$. Thus if M_p is the field generated by $\bigcup_{n(q)\geq 1,\, q\neq p}\mathsf{Q}(\mu_q)$, then $M_p\cap \mathsf{Q}(\mu_p)=\mathsf{Q}$ and it follows by statement (k) of chapter VII of [4] that if M is the field generated by $\bigcup_{p\,\text{odd}}\mathsf{Q}(\mu_p)$ then

$$\mathrm{Gal}(M\,|\,\mathsf{Q}) = \textstyle\prod_p \mathrm{Gal}(\mathsf{Q}(\mu_p)\,|\,\mathsf{Q}) = \prod_p \mathsf{Z}/2^{n(p)}\,.$$

Let K be any algebraic number field; then $\mathrm{Gal}(KM\,|\,K)=\mathrm{Gal}(M\,|\,K\cap M)$ which is a subgroup of $\mathrm{Gal}(M\,|\,\mathsf{Q})$ of finite index. It follows that there is a subfield of KM which has any direct product of a countable number of two groups as quotient group. Thus A is a quotient group. The result follows since $HK\,|\,K$ is abelian with quotient group Z_2.

The above construction gives the maximal abelian quotient group of $\mathrm{PG}(\mathsf{Q})$, since any abelian extension of Q is contained in a cyclotomic extension. In particular there is a unique subfield of $\mathrm{PG}(\mathsf{Q})$ with galois group Z_2; it is precisely H.

$\mathrm{PG}(\mathsf{Q})$ has all possible groups of order eight as quotient groups. Since $\mathrm{PG}(\mathsf{Q})$ has all abelian groups of order 2^n as quotient groups we need only be concerned with the dihederal group and the quaternion group.

(i) Dihederal: Let g,f be positive integers with $g^2>f$ and none of $g^2-f, f, g^2/f-1$ squares. If

$$x = e\sqrt{f}+(g+\sqrt{f})^{\frac{1}{2}}$$

then $\mathrm{Gal}(\mathsf{Q}(x)\,|\,\mathsf{Q})$ is dihederal (see Siedelmann [7]). To show that $x\in \mathsf{Q}_p$ we need only show that $g+\sqrt{f}$ is a sum of squares in $\mathsf{Q}(\sqrt{f})$.

$$\begin{aligned} g+\sqrt{f} &= 2g(\tfrac{1}{2}+\sqrt{f}/2g)^2+g/2-f/2g \\ &= 2g(\tfrac{1}{2}+\sqrt{f}/2g)^2+2g(g^2-f)(1/2g)^2; \end{aligned}$$

since $2g$ and $2g(g^2-f)$ are positive integers this is a sum of squares.

(ii) Quaternions: $\mathsf{Q}((1+1/\sqrt{3})(1+1/\sqrt{2}))^{\frac{1}{2}}$ is contained in Q_p and has the quaternions as Galois group. The conjugate roots are

$$\begin{aligned} x_0 &= ((1+1/\sqrt{3})(1+1/\sqrt{2}))^{\frac{1}{2}}, & x_1 &= ((1-1/\sqrt{3})(1+1/\sqrt{2}))^{\frac{1}{2}}\,, \\ x_2 &= ((1+1/\sqrt{3})(1-1/\sqrt{2}))^{\frac{1}{2}}, & x_3 &= ((1-1/\sqrt{3})(1-1/\sqrt{2}))^{\frac{1}{2}}\,, \end{aligned}$$
$$-x_0,\ -x_1,\ -x_2 \text{ and } -x_3\,.$$

If $\sigma(x_0)=x_1$ and $\tau(x_0)=x_3$ then it is easy to show that $\sigma^2=\tau^2$, $\sigma^4=\mathrm{id}$ and $\sigma\tau=\tau\sigma^3$. Since $1+1/\sqrt{3}$ is positive in all orderings of $\mathsf{Q}(1/\sqrt{3})$ it is a sum of squares in this field; thus $\mathsf{Q}((1+1/\sqrt{3})^{\frac{1}{2}})$ is in Q_p; similarly so is $\mathsf{Q}((1+1/\sqrt{2})^{\frac{1}{2}})$.

If K is any C_1 field i.e. every homogeneous polynomial in n variables of degree less than n has a non trivial zero, then $\mathrm{cd}_2(K) \leqq 1$ by corollary 4.3, page 269 of [5]. Consequently if A is any algebraicly closed field, $\mathrm{PG}(A(X))$ is a free pro-2-group. The rank of the group is the number of square classes i.e. $A(X)^*/(A(X)^*)^2$.

REFERENCES

1. E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.
2. J. Diller and A. Dress, *Zur Galoistheorie Pythagoreischer Korper*, Arch. Math. 16 (1965), 148–152.
3. S. Lang, *Algebra*, Addison-Wesley, Reading, 1965.
4. P. Ribenboim, *L'Arithmetique des Corps*, Hermann, Paris 1972.
5. L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's University, Kingston, 1970.
6. O. Schilling, *The theory of valuations* (Mathematical Surveys 4), American Mathematical Society, New York, 1950.
7. F. Seidelmann, *Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitatsbereich*, Math. Ann. 78 (1918), 230–233.
8. J. P. Serre, *Cohomologie Galoisienne* (Lecture Notes in Mathematics 5), Springer-Verlag, Berlin-Heidelberg-New York, 1964.

QUEEN'S UNIVERSITY, KINGSTON, ONTARIO, CANADA