PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 4, April 1995

ABELIAN SUBGROUPS OF PRO-2 GALOIS GROUPS

IDO EFRAT

(Communicated by Lance W. Small)

ABSTRACT. Let $a(K)$ be the maximal cardinality $|I|$ such that $\mathbb{Z}_2^I$ is a closed subgroup of the maximal pro-2 Galois group of a field K. We prove estimates on $a(K)$ conjectured by Ware.

Let K be a field of characteristic $\neq 2$, and let $K(2)$ be its maximal pro-2 Galois extension. Thus, $K(2)$ is obtained from K by repeatedly adjoining all square roots. Let $G_K(2)$ be the Galois group $\mathrm{Gal}(K(2)/K)$. In [11] Ware defines the a-invariant $a(K)$ of K to be the maximal rank (possible ∞) of closed subgroups of $G_K(2)$ which are torsion-free and abelian. Note that by Pontryagin duality, such subgroups are of the form $\mathbb{Z}_2^I$ for some index set I. Another closely related invariant of K is its (absolute) stability index $\mathrm{st}(K)$, defined as the minimal positive integer m (∞ if no such m exists) such that $I^{m+1}(K) = 2I^m(K)$, where $I(K)$ is the fundamental ideal of the Witt ring $W(K)$ of K. In the present note we prove the following three conjectures raised in [11]:

Theorem. (I) *If K is formally real, then* $a(K) \leq \mathrm{rank}\, G_K(2) - 1$.
(II) *For every finite extension E/K of fields,* $a(K) \leq a(E)$.
(III) $a(K) \leq \mathrm{st}(K)$.

(With regard to conjecture (I), the conjecture in [11] is in fact only that $a(K) \leq \mathrm{rank}\, G_K(2)$; this slightly weaker inequality is proved in [11, Corollary 5, p. 992] for nonformally real fields.)

Our proofs are based on valuation-theoretic techniques. For convenience, we recall the following notions and facts from [2, p. 151]: A valued field (K, v) is 2-*henselian* if v has a unique extension to $K(2)$. Equivalently, Hensel's lemma holds for polynomials that split completely in $K(2)$. An arbitrary valued field (K, v) has an immediate 2-extension $(\widehat{K}, \hat{v})$ which is 2-henselian and which uniquely embeds in every 2-henselian extension (L, u) of (K, v) contained in $K(2)$. In fact, $\widehat{K}$ is the decomposition field of any extension of v to $K(2)$. An extension $(\widehat{K}, \hat{v})$ as above is called a 2-*henselization* of (K, v). We denote $q(K) = (K^\times : (K^\times)^2)$. To avoid notational inconsistency, we do not distinguish here and in the sequel between different infinite cardinalities.

Received by the editors July 9, 1993.
1991 *Mathematics Subject Classification*. Primary 12F12, 12J10.

Lemma 1. *Let* (K, v) *be a* 2*-henselian field with value group* Γ *and residue field* $\overline{K}$ *of characteristic* $\neq 2$. *Then*:

(a) $G_K(2) \cong A \rtimes G_{\overline{K}}(2)$, *where* A *is a torsion-free abelian group of rank* $\dim_{\mathbf{F}_2} \Gamma/2\Gamma$.

(b) *If* $\overline{K}$ *contains all roots of unity of* 2*-power order over its prime field, then* $G_K(2) \cong A \times G_{\overline{K}}(2)$ *with* A *as above.*

(c) $q(K) = q(\overline{K})|\Gamma/2\Gamma|$.

Proof. (a) is well known (see, e.g., [4, §§19, 20]). (b) follows from (a) and from [6, Theorem 2.2(ii)]. For (c), take a subset T of $K^\times$ such that $v(t)$, $t \in T$, represent the distinct cosets of $\Gamma/2\Gamma$. By Hensel's lemma, the 1-units of v are squares. Every element $x \in K^\times$ can be written as $x = \alpha t y^2$, where α is a unit of v, $t \in T$, and $y \in K$. This induces a bijection $K^\times/(K^\times)^2 \cong \overline{K}^\times/(\overline{K}^\times)^2 \times T$, whence the assertion. □

Our main tool is the following valuation-theoretic description of the a-invariant:

Proposition 2. *Given a field* K *with* $a(K) \geq 2$ *there exists a valuation* v *on* K *whose residue field* $\overline{K}$ *and value group* Γ *satisfy*:

(i) $\operatorname{char} \overline{K} \neq 2$;

(ii) $a(K) = \log_2 |\Gamma/2\Gamma| + 1$ (*in particular,* $\Gamma \neq 2\Gamma$);

(iii) $a(\widehat{K}) = a(K)$ *for any* 2*-henselization* $\widehat{K}$ *of* K;

(iv) $\overline{K}(2)/\overline{K}(\mu)$ *is infinite, where* μ *is the group of all roots of unity of* 2*-power order over the prime field of* $\overline{K}$.

Proof. We first observe that $\operatorname{char} K \neq 2$. For otherwise $\operatorname{cd}(G_K(2)) \leq 1$ [9, II-4, Proposition 3]. Since $\operatorname{cd}(\mathbb{Z}_2^I) = |I|$ (use, e.g., [9, I-32, Proposition 22]), this implies that $a(K) \leq 1$, contrary to the assumption.

Now let L be the fixed field of a torsion-free abelian closed subgroup of $G_K(2)$ of maximal rank. Write $G_L(2) \cong \mathbb{Z}_2^I \times \mathbb{Z}_2$ with $|I| \geq 1$. By [6, Theorem 2.5] (and its proof), L has a 2-henselian valuation u whose residue field $\overline{L}$ satisfies $\operatorname{char} \overline{L} \neq 2$ and $G_{\overline{L}}(2) \cong \mathbb{Z}_2$. By [10, Theorem 3.6], L contains all roots of unity of 2-power order over its prime field. Hence, so does $\overline{L}$. Let v be the restriction of u to K, and let $(\widehat{K}, \hat{v})$ be a 2-henselization of (K, v). We may take $\widehat{K} \subseteq L$. Let $v(2)$ be the unique extension of $\hat{v}$ to $K(2)$, and let $\overline{K}$, $\overline{K(2)}$ be the residue fields of (K, v) and $(K(2), v(2))$, respectively. Since $\overline{L}/\overline{K}$ is an algebraic extension, $\operatorname{char} \overline{K} \neq 2$. Therefore, the 2-extension $\overline{K(2)}/\overline{K}$ is separable. Clearly, $\overline{K(2)}$ is quadratically closed. Thus $\overline{K(2)} = \overline{K}(2)$. Denoting the inertia field of $(K(2), v(2))/(\widehat{K}, \hat{v})$ by K^T we obtain from [4, Theorem 19.6] that

$$\operatorname{Gal}(K^T/\widehat{K}) \cong \operatorname{Aut}(\overline{K(2)}/\overline{K}) = G_{\overline{K}}(2).$$

Next let $E = L \cap K^T$. It is 2-henselian with respect to the unique extension of $\hat{v}$ [2, Proposition 1.6] and has value group Γ and residue field $\overline{L}$. By Lemma 1(b), $G_E(2)$ is a torsion-free abelian pro-2 group of rank $\log_2 |\Gamma/2\Gamma| + 1$. As $K \subseteq \widehat{K} \subseteq E \subseteq L$ and $a(K) = a(L)$, we have

$$a(K) = a(\widehat{K}) = a(E) = \log_2 |\Gamma/2\Gamma| + 1,$$

proving (ii) and (iii).

Finally, (iv) follows from the fact that $\overline{K}(\mu) \subseteq \overline{L} \subset \overline{K}(2)$, and $G_{\overline{L}}(2) \cong \mathbb{Z}_2$. □

Remarks. (1) Given a field K, with $a(K) \geq 2$, one in general does not have a valuation on K with value group Γ satisfying $a(K) = \log_2 |\Gamma/2\Gamma|$. For example, let $\mathbb{Q}_{ab}$ be the maximal pro-abelian extension of $\mathbb{Q}$ and let E be any algebraic extension of $\mathbb{Q}_{ab}$ with absolute Galois group $\mathbb{Z}_2$. The field $K = E((t))$ is henselian with respect to its natural valuation u. By Lemma 1(b), $G_K(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, hence $a(K) = 2$. We show that for every nontrivial valuation v on K with value group Γ, $|\Gamma/2\Gamma| \leq 2$. Indeed, if v and u are independent, then the (ordinary) henselization of K with respect to u is the algebraic closure $\widetilde{K}$ [5, Corollary 2.4], so Γ is in this case divisible. Suppose on the other hand that v and u are dependent and distinct. Since the value group $\mathbb{Z}$ of u has no nontrivial isolated subgroups, there are no proper nontrivial coarsenings of u [1, Chapter VI, §4.3, Proposition 4]. Therefore, v is finer then u. Let v^0 be the valuation induced by v on the residue field E of u, and let Γ_0 be its value group. One has a short exact sequence:

$$0 \to \Gamma_0 \to \Gamma \to \mathbb{Z} \to 0$$

[1, Chapter VI, §4.3, Remark]. The restriction of v_0 to $\mathbb{Q}$ is p-adic for some prime p. Since $\sqrt[n]{p} \in \mathbb{Q}_{ab} \subseteq E$ for all $n \geq 1$, the group Γ_0 is divisible. Therefore, $\Gamma/2\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, as desired.

(2) For every valuation v on K with value group Γ and residue characteristic $\neq 2$, $\log_2 |\Gamma/2\Gamma| \leq a(K)$ [11, Corollary 2(i), p. 990].

Proof of (I). By Kummer theory and [9, I-38, Corollary],

$$\log_2 q(K) = \dim_{\mathbb{F}_2} \operatorname{Hom}(G_K(2), \mathbb{Z}/2\mathbb{Z}) = \operatorname{rank} G_K(2).$$

We therefore need to show that $a(K) \leq \log_2 q(K) - 1$ for K formally real. This is trivial when $q(K) = \infty$. Suppose then that $q(K) < \infty$. We prove the assertion by induction on $q(K)$. The case $a(K) = 0$ is clear. If $a(K) = 1$, then $q(K) \geq 4$ by [11, Example (1)], as required. We may therefore assume that $a(K) \geq 2$. Let v, $\overline{K}$, and Γ be as in Proposition 2, and let $(\widehat{K}, \hat{v})$ be a 2-henselization of (K, v). Then $\widehat{K} = K\widehat{K}^2$ (see, e.g., [3, Lemma 2.4(a)]). Therefore, the natural homomorphism

$$\Lambda\colon K^\times/(K^\times)^2 \to \widehat{K}^\times/(\widehat{K}^\times)^2$$

is surjective, so one of the following holds:

Case (1): Λ *is not injective.* Then $2q(\widehat{K}) \leq q(K)$. If $\widehat{K}$ is formally real, we may therefore apply the induction hypothesis to obtain that $a(\widehat{K}) \leq \log_2 q(\widehat{K}) - 1$. If $\widehat{K}$ is not formally real, then we still have $a(\widehat{K}) \leq \log_2 q(\widehat{K})$, by [11, Corollary 5, p. 992]. As $a(K) = a(\widehat{K})$, we conclude that $a(K) \leq \log_2(\widehat{K}) \leq \log_2 q(K) - 1$, as required.

Case (2): Λ *is an isomorphism.* Let M be the maximal ideal of the valuation ring of v. By Hensel's Lemma, $1+M \subseteq \widehat{K}^2 \cap K = K^2$. This implies that (K, v) is 2-henselian [7, Lemma 3.14], i.e., $\widehat{K} = K$. We have $q(\overline{K}) < (\Gamma\colon 2\Gamma)q(\overline{K}) = q(K)$, by Lemma 1(c). Moreover, $\overline{K}$ is formally real [7, Lemma 3.15]. From the induction hypothesis we therefore get $a(\overline{K}) \leq \log_2 q(\overline{K}) - 1$. Conclude from [11, Corollary 1, p. 990] that

$$a(K) \leq \log_2 |\Gamma/2\Gamma| + a(\overline{K}) \leq \log_2 |\Gamma/2\Gamma| + \log_2 q(\overline{K}) - 1 = \log_2 q(K) - 1,$$

completing the induction. □

Remarks. (1) Ware [11, Remark, p. 992] proves (I) for K (real-)pythagorean and shows that in general $a(K) \leq 2\log_2(K) - 2$.

(2) The bound $a(K) \leq \log_2 q(K) - 1$ for K formally real is sharp. For example, a repeated application of Lemma 1(a) shows that $K = \mathbb{R}((t_1))\cdots((t_n))$ has $G_K(2) \cong \mathbb{Z}_2^n \rtimes (\mathbb{Z}/2\mathbb{Z})$, hence $a(K) = \log_2 q(K) - 1 = n$.

(3) If K is not formally real, then in general one cannot improve the bound $a(K) \leq \log_2 q(K)$ given in [11, Corollary 5, p. 992]. E.g., $K = \widetilde{\mathbb{Q}}((t_1))\cdots((t_n))$ has $a(K) = \log_2 q(K) = n$.

(4) Denote the maximal rank of torsion-free abelian closed subgroups of a pro-2 group G by $a(G)$. The inequality $a(G) \leq \operatorname{rank} G$, although valid for maximal pro-2 Galois groups of fields (by (I) and [11, Corollary 5, p. 992]), does not hold for arbitrary pro-2 groups. For example, the wreath product $G = \mathbb{Z}_2 \wr (\mathbb{Z}/4\mathbb{Z})$ has rank 2, yet it has $\mathbb{Z}_2^4$ as an open subgroup.

For the next proof we need an almost trivial yet important observation:

Lemma 3. *Let Γ be a subgroup of a finite index of a torsion-free abelian group Δ. Then* $(\Delta\colon 2\Delta) = (\Gamma\colon 2\Gamma)$.

Proof. Since Δ is torsion-free, $\Delta/\Gamma \cong 2\Delta/2\Gamma$ naturally. The assertion therefore follows from the equalities

$$(\Delta\colon 2\Delta)(2\Delta\colon 2\Gamma) = (\Delta\colon 2\Gamma) = (\Delta\colon \Gamma)(\Gamma\colon 2\Gamma). \quad □$$

Proof of (II). If $a(E) = 0$, then $[E(2)\colon E] \leq 2$ by [11, Example (1)], whence $[K(2)\colon K] < \infty$ and we get $a(K) = 0$. We may therefore assume that $a(K) \geq 2$. Let v, Γ, $\overline{K}$, and μ be as in Proposition 2. Also let u be an extension of v to E, let $\overline{E}$ be the residue field of (E, u), and let Δ be its value group. Fix a 2-henselization $\widehat{E}$ of (E, u). Since $\overline{E}/\overline{K}$ and, hence, $\overline{E}(\mu)/\overline{K}(\mu)$ are finite extensions and since $\overline{E}(2)/\overline{K}(\mu)$ is infinite, $\overline{E}(\mu) \neq \overline{E}(2)$. By [11, Theorem 1(i)], $a(\widehat{E}) = \log_2 |\Delta/2\Delta| + a(\overline{E})$. Since $\overline{K}(2)/\overline{K}$ is an infinite extension, so is $\overline{E}(2)/\overline{K}$, hence so is $\overline{E}(2)/\overline{E}$. In particular, $1 \leq a(\overline{E})$, by [11, Example (1)), p. 985] again. From this and from Lemma 3 we deduce:

$$a(K) = \log_2 |\Gamma/2\Gamma| + 1 \leq \log_2 |\Delta/2\Delta| + a(\overline{E}) = a(\widehat{E}) \leq a(E). \quad □$$

Remark. The inequality (II) holds also when $\operatorname{char} K = 2$. Indeed, as observed at the beginning of the proof of Proposition 2, this implies that $a(K) \leq 1$. Moreover, $a(E) = 0$ if and only if E is quadratically closed. But in this case we obviously have $a(K) = 0$ as well.

Proof of (III). If $\operatorname{st}(K) = 0$, then K is quadratically closed and we are done. We may therefore assume that $a(K) \geq 2$. Let v, Γ, and $\overline{K}$ be as in Proposition 2, and choose a subset T of $K^\times$ such that the cosets of $v(t)$, $t \in T$, form a linear basis of $\Gamma/2\Gamma$ over $\mathbb{F}_2$. Thus, $a(K) = \log_2 |\Gamma/2\Gamma| + 1 = |T| + 1$. Since $\overline{K}$ is not quadratically closed, there exists a v-unit α in K whose residue $\overline{\alpha}$

is not in $\overline{K}^2$. For any finite subset T_0 of T having m elements, consider the $(m+1)$-Pfister form $\varphi_{T_0} = \langle\langle \alpha \rangle\rangle \otimes \bigotimes_{t\in T_0} \langle\langle t \rangle\rangle$. Its similarity class is in $I^{m+1}(K)$. But all its nonzero residue forms (cf. [8, p. 136]) are $\langle\langle \overline{\alpha} \rangle\rangle$ and, hence, are not in $2W(\overline{K})$. It follows that $\varphi_{T_0} \notin 2I^m(K)$, so $m < \mathrm{st}(K)$. Conclude that $a(K) = |T| + 1 \leq \mathrm{st}(K)$. □

Acknowledgments

This note was written during the author's stay at Konstanz University as an Alexander von Humboldt fellow. He thanks Jochen Koenigsmann for very helpful discussions on this subject.

References

1. N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1972.
2. L. Bröcker, *Characterization of fans and herditarily pythagorean fields*, Math. Z. **151** (1976), 149–163.
3. I. Efrat, *Free product decompositions of Galois groups over pythagorean fields*, Comm. Algebra **21** (1993), 4495–4511.
4. O. Endler, *Valuation theory*, Springer, Berlin, 1972.
5. A. Engler, *Fields with two incomparable henselian valuation rings*, Manuscripta Math. **23** (1977), 373–385.
6. B. Jacob and R. Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings*, Math. Z. **200** (1989), 379–396.
7. T. Y. Lam, *Orderings, valuations and quadratic forms*, Conf. Board Math. Sci., vol. 52, Amer. Math. Soc., Providence, RI, 1983.
8. W. Scharlau, *Quadratic and Hermitian forms*, Springer, Berlin, 1985.
9. J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math., vol. 5, Springer, Berlin, 1965.
10. R. Ware, *When are Witt rings groups rings*? II, Pacific J. Math. **76** (1978), 541–564.
11. ———, *Stability in Witt rings and abelian subgroups of pro-2-Galois groups*, Rocky Mountain J. Math. **19** (1989), 985–995.

Fakultät für Mathematik, Universität Konstanz, Postfach 5560, D-7750 Konstanz, Germany