MR2607857 (Review) 11A15 (11R21)

Balasubramanian, R. [Balasubramanian, Ramachandran] (6-MATSCI);
Luca, F. (MEX-NAM-IM); **Thangadurai, R.** (6-HCRI)

On the exact degree of $\mathbb{Q}(\sqrt{a_1},\sqrt{a_2},\ldots,\sqrt{a_\ell})$ over $\mathbb{Q}$. (English summary)

Proc. Amer. Math. Soc. **138** (2010), *no. 7,* 2283–2288.

Let $S = \{a_1, a_2, \ldots, a_\ell\}$ be a finite set of nonzero integers. From basic field theory it is known that the degree of the field

$$\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_\ell})$$

is 2^t for some integer $0 \leq t \leq \ell$, depending on the algebraic cancellations among the a_i.

The authors prove in this paper that $t = \ell - k$, where 2^k is the sum of the number of subsets of S of even cardinality the product of whose elements is a square and the number of subsets of odd cardinality the product of whose elements is a square. The theorem is proved using density arguments and Chebotarev's Density Theorem. The problem of determining t is reduced to the problem of generating complete factorings of the a_i followed by some linear algebra on a matrix of size $\ell \times r$, where r is the total number of primes used in factoring the a_i.

Reviewed by *Duncan A. Buell*

References

1. M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith., **15** (1968/69), 91–115. MR0244150 (39 #5467)
2. C. S. Abel-Hollinger and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over multiquadratic fields*, Number-theoretic and algebraic methods in com- puter science (Moscow, 1993), 69-87, World Sci. Publ., River Edge, NJ, 1995. MR1377742 (97e:11060)
3. M. Laska and M. Lorenz, *Rational points on elliptic curves over* Q *in elementary abelian* 2*-extensions of* Q, J. Reine Angew. Math., **355** (1985), 163–172. MR0772489 (86d:11048)
4. K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith., **29** (1976), 113–146. MR0396448 (53 #313)
5. S. Wright, *Patterns of quadratic residues and nonresidues for infinitely many primes*, J. Number Theory, **123** (2007), 120–132. MR2295434 (2007j:11007)
6. S. Wright, *A combinatorial problem related to quadratic non-residue modulo p*, Ars Combinatorica, to appear.

Note: This list, extracted from the PDF form of the original paper, may contain data conversion errors, almost all limited to the mathematical expressions.