A NOTE ON COMMON INDEX DIVISORS

L. CARLITZ

1. **Introduction.** A prime q *is a common index divisor* of the algebraic number field K if q divides the quotient $d(\omega)/d$ for all integers ω of K, where $d(\omega)$ is the discriminant of ω and d is the discriminant of the field. A necessary condition is that q be less than the degree of the field [7].

Let the prime $p\equiv 1 \pmod 3$ and let $Z=k(\zeta)$ be the field generated by ζ, a primitive pth root of unity; also let C_3 denote the cubic subfield of Z; k stands for the rational field. Then Hensel [1, p. 284] proved that the prime 2 is a common index divisor of C_3 if and only if $p=a^2+27b^2$.

In the present note we shall prove several theorems of a similar kind. For example let $p\equiv 1 \pmod 4$ and let C_4 denote the quartic subfield of Z. Then 2 is a common index divisor of C_4 if and only if $p\equiv 1 \pmod 8$. The condition that 3 be a common index divisor is somewhat more complicated, namely, let $p=a^2+b^2$, $a\equiv 1$, $b\equiv 0 \pmod 2$. Then for $p\equiv 1 \pmod 8$ it is necessary and sufficient that $3\mid b$, while for $p\equiv 5 \pmod 8$ it is necessary and sufficient that $3\mid a$.

2. We recall the following criterion [1, p. 276] for a common index divisor in a field K. Let

$$q = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}, \qquad N\mathfrak{q}_i = q^{f_i}, \tag{2.1}$$

be the prime-ideal decomposition of q in K, let $g(f)$ denote the number of $\mathfrak{q}$'s of degree f in (2.1), and let $\psi(f)$ be the number of primary irreducible polynomials of degree f in $GF[q, x]$. Then q is a common index divisor of K if and only if $\psi(f_i)<g(f_i)$ for at least one value of i.

In the next place we require the following decomposition rule due to Dedekind [4]. For simplicity we consider only primes not contained in the discriminant.

Decomposition Rule. Let Z_m be the field generated by a primitive mth root of unity and K any subfield. Let the group of Z_m be represented by a reduced residue system $(\text{mod } m)$ and let (h) denote the subgroup corresponding to K. If $q\nmid m$, let f be the smallest positive exponent such that

Presented to the Society, April 26, 1952; received by the editors January 15, 1952.

(2.2) $$q^f \equiv (h) \pmod{m},$$

that is, to one of the numbers of (h). Then the prime-ideal decomposition of q in K is given by

(2.3) $$q = \mathfrak{q}_1 \cdots \mathfrak{q}_e, \qquad N\mathfrak{q}_i = q^f.$$

3. By means of the decomposition rule it is very easy to determine the prime-ideal factorization of the prime 2 in the field C_4. In the first place the subgroup (h) is evidently the set of biquadratic residues (mod p). Hence the condition (2.2) becomes

(3.1) $$2^{f(p-1)/4} \equiv 1 \pmod{p}.$$

Now on the other hand the only possible factorizations of 2 in C_4 are (i) $2=\mathfrak{q}$, (ii) $2=\mathfrak{q}_1\mathfrak{q}_2$, (iii) $2=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$, where $\mathfrak{q}$, $\mathfrak{q}_i$ denote prime ideals, in (ii) $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are of degree 2, and in (iii) the $\mathfrak{q}_i$ are of degree 1. Since there is but one irreducible quadratic (mod 2) and but two linear polynomials, it follows from the criterion quoted above that in either case (ii) or (iii), 2 is a common index divisor. Clearly case (i) will occur if and only if $f=4$ in (3.1); since $f=1$ or 2 implies 2 a quadratic residue (mod p), case (i) will occur only if 2 is a nonresidue, that is, $p\equiv 5 \pmod{8}$. Thus case (ii) or (iii) occurs only when $p\equiv 1 \pmod{8}$. This proves:

THEOREM 1. *The prime 2 is a common index divisor of C_4 if and only if $p\equiv 1 \pmod{8}$.*

By the same argument 3 is a common index divisor of C_4 if and only if 3 is a biquadratic residue of p. To get a more explicit criterion we apply the biquadratic reciprocity theorem in $k(i)$ [2, p. 168]. Let $p=(a+bi)(a-bi)$, where $a\equiv 1$, $b\equiv 0 \pmod{2}$. Then $(-3/(a+bi))_4 = +1$ if and only if $3|b$, while $(-3/(a+bi))_4=-1$ if and only if $3|a$. Thus for $p\equiv 1 \pmod{8}$, 3 is a biquadratic residue only if $3|b$; for $p\equiv 5 \pmod{8}$, 3 is a biquadratic residue only if $3|a$.

THEOREM 2. *Let $p=a^2+b^2$, $a\equiv 1$, $b\equiv 0 \pmod{2}$. Then the prime 3 is a common index divisor of C_4 if and only if $3|b$ for $p\equiv 1 \pmod{8}$, $3|a$ for $p\equiv 5 \pmod{8}$.*

4. Let $ef'=p-1$ and let C_e denote the cyclic subfield of Z of degree e. Then it is evident from the decomposition rule that a *sufficient* condition that the prime $q<e$ be a common index divisor of C_e is furnished by

(4.1) $$q^{f'} \equiv 1 \pmod{p}.$$

If e is a prime, then (4.1) is also a necessary condition. Thus for $e=3$, for example, Hensel's criterion is indeed equivalent to (4.1) with $q=2$. For $e=5$ no very simple explicit results are available; see however [6] for the quintic character of 2 and 3. These results may be interpreted to give necessary and sufficient conditions that 2 or 3 be a common index divisor of C_5.

We may however deduce simple explicit results in one or two cases by combining the criteria already obtained. For example in C_6 the factorization $2=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ or $2=\mathfrak{q}_1\cdots\mathfrak{q}_6$ imply 2 a common index divisor, while $2=\mathfrak{q}$ or $2=\mathfrak{q}_1\mathfrak{q}_2$ imply the contrary. Now it is evident that the first two factorizations can occur only if $2=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in C_3, that is, 2 is a common index divisor of C_3. Thus Hensel's criterion applies and we have:

THEOREM 3. *Let* $p\equiv 1 \pmod 6$. *Then 2 is a common index divisor of* C_6 *if and only if* $p=a^2+27b^2$, *that is, if and only if 2 is a common index divisor of* C_3.

As for the prime 3, it is evident that it will be a common index divisor of C_6 if and only if $3=\mathfrak{q}_1\cdots\mathfrak{q}_6$. This requires $3=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in C_3 and $3=\mathfrak{p}_1'\mathfrak{p}_2'$ in C_2. The factorization in [5, p. 236]

$$C_2 = k((-1)^{(p-1)/2}p)^{1/2}$$

holds provided $(-1)^{(p-1)/2}p\equiv 1 \pmod 3$; since $p\equiv 1 \pmod 3$, this condition reduces to simply $p\equiv 1 \pmod 4$. On the other hand, by the decomposition rule, the factorization in C_3 requires that 3 be a cubic residue of p. Let $p=a^2-ab+b^2$, $a\equiv -1$, $b\equiv 0 \pmod 3$. Then it is well known that 3 is a cubic residue (mod p) if and only if $9\mid b$ (see [2, p. 223]). We thus get:

THEOREM 4. *Let* $p\equiv 1 \pmod 6$ *and put* $p=a^2-ab+b^2$, *where* $a\equiv -1$, $b\equiv 0 \pmod 3$. *Then 3 is a common index divisor of* C_6 *if and only if* $9\mid b$ *and* $p\equiv 1 \pmod 4$.

We omit the discussion of criteria corresponding to $q=5$.

5. Turning to C_{12}, the factorization (i) $2=\mathfrak{q}_1\cdots\mathfrak{q}_4$, each $\mathfrak{q}$ of degree 3, (ii) $2=\mathfrak{q}_1\cdots\mathfrak{q}_6$, each $\mathfrak{q}$ of degree 2, (iii) $2=\mathfrak{q}_1\cdots\mathfrak{q}_{12}$, each $\mathfrak{q}$ of degree 1, are the only ones that imply 2 a common index divisor. Now case (i) occurs if and only if 2 factors completely in C_4, that is, if 2 is a biquadratic residue of p. The condition for this (see [2, p. 236]) can be put as follows. Let $p=a^2+b^2$, $a\equiv 1$, $b\equiv 0 \pmod 2$. Then b must be divisible by 8.

(ii) requires that $2=\mathfrak{p}_1\mathfrak{p}_2$ in C_4 and $2=\mathfrak{p}_1'\mathfrak{p}_2'\mathfrak{p}_3'$ in C_3; hence it is necessary that $p\equiv 1 \pmod 8$ and that Hensel's criterion be satisfied.

(iii) requires that $2=\mathfrak{p}_1 \cdots \mathfrak{p}_4$ in C_4 and $2=\mathfrak{p}_1'\mathfrak{p}_2'\mathfrak{p}_3'$ in C_3; again $p\equiv 1 \pmod 8$ and Hensel's criterion must be satisfied.

Combining the several possibilities we get:

THEOREM 5. *Let* $p\equiv 1 \pmod{12}$. *Then* 2 *is a common index divisor of* C_{12} *if and only if*

(a) $$p = a^2 + b^2, \qquad b \equiv 0 \pmod 8,$$

or

(b) $$p \equiv 1 \pmod 8 \quad \textit{and} \quad p = u^2 + 27v^2.$$

We omit the discussion of criteria that 3 be a common index divisor of C_{12}.

6. Finally we consider C_8, $q=2$. The only factorizations to examine are (i) $2=\mathfrak{q}_1 \cdots \mathfrak{q}_4$, each $\mathfrak{q}$ of degree 2, (ii) $2=\mathfrak{q}_1 \cdots \mathfrak{q}_8$, each $\mathfrak{q}$ of degree 1. It is clear from the decomposition rule that case (i) or (ii) will occur if and only if 2 is a biquadratic residue of p. Hence by the discussion of case (i) of the previous proof we have:

THEOREM 6. *Let* $p\equiv 1 \pmod 8$ *and put* $p=a^2+b^2$, $b\equiv 0 \pmod 2$. *Then* 2 *is a common index divisor of* C_8 *if and only if* $b\equiv 0 \pmod 8$.

As for $q=3$, the condition is that 3 be a biquadratic residue of p. Hence comparing with the proof of Theorem 2, we have:

THEOREM 7. *Let* $p\equiv 1 \pmod 8$ *and put* $p=a^2+b^2$, $a\equiv 1$, $b\equiv 0 \pmod 2$. *Then* 3 *is a common index divisor of* C_8 *if and only if* $3\mid b$. *Thus* 3 *is a common index divisor of* C_8 *if and only if it is a common index divisor of* C_4.

For other theorems on common index divisors in abelian fields see [3, pp. 131–136]. Thus in particular 2 is always a common index divisor of noncyclic abelian quartic fields of odd discriminant. Indeed by Theorem 6 of [3] if the abelian field K is of degree p^n and type $(1, \cdots, 1)$ and if $q\nmid d(K)$ and $q\leqq p^{n/p}$, then q is certainly a common index divisor of K. We also remark that for the noncyclic quartic field

$$K = k(p_1^{1/2}, q_1^{1/2}), \; p_1 = (-1)^{(p-1)/2}p, \; q_1 = (-1)^{(q-1)/2},$$

where p, q are distinct primes >3, the prime 3 will be a common index divisor if and only if $p_1\equiv q_1\equiv 1 \pmod 3$. For by the decomposition rule (§2) the factorization $3=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$ will occur if and only if $3\equiv a^2 \pmod{pq}$, which is readily seen to be equivalent to the stated condition. Other theorems of this kind are readily obtained.

References

1. P. Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, Leipzig, 1905.

2. ———, *Die Lehre von der Kreisteilung*, Leipzig and Berlin, 1921.

3. L. Carlitz, *On abelian fields*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 122–136.

4. R. Dedekind, *Sur la théorie des nombres complexes idéaux*, Gesammelte Mathematische Werke, vol. 1, Braunschweig, 1930, pp. 233–235.

5. R. Fueter, *Synthetische Zahlentheorie*, Berlin and Leipzig, 1925.

6. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. vol. 18 (1951) pp. 11–18.

7. E. v. Zylinski, *Zur Theorie der ausserwesentliche Diskriminantenteiler algebraischer Körper*, Math. Ann. vol. 73 (1913) pp. 273–274.

Duke University