ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 27, Number 4, Fall 1997

COMPARING THE UNIT GROUPS OF TWO ORDERS IN A NUMBER FIELD

JOHN WOLFSKILL

ABSTRACT. Let $R \subset S$ be two orders in a number field, and let E_R and E_S be their unit groups. In this paper we bound the order of the quotient unit group E_S/E_R in terms of the order of the quotient ring S/R.

1. Introduction. Let R and S be two orders in a number field K, and let E_R and E_S be their unit groups. Then S/R and E_S/E_R are both finite. The object of this paper is to bound $|E_S/E_R|$ in terms of $|S/R|$, continuing the work of [**2**]. In [**2**] this problem is solved for the case that S and R have just one generator different in their Z-bases; so S/R is cyclic as a Z-module. The results are as follows: if $S/R \simeq Z_p$, then E_S/E_R is cyclic of order $\leq p+1$ (actually, the order is a divisor of $p-1$, p or $p+1$). If $S/R \simeq Z_{p^r}$ with $r > 1$, the group structure of E_S/E_R may be more complicated, but its order is bounded by $p^{r-1}(p+1)$.

To treat the general case, where S/R may have an arbitrary number of generators, the first step is to observe that the extension S/R can be considered as a sequence of extensions in which only one prime is involved in the denominators at each step. Thus we may assume that S/R, additively, is a p-group.

It will be shown that when S/R is a p-group, it may be broken down into a sequence of extensions of type $Z_p \oplus \cdots \oplus Z_p$ for a varying number of summands. For an extension of this basic type, the quotient unit group may be noncyclic, in contrast to the situation with only one generator. An example to illustrate this is given after Theorem 1. Therefore, we will focus solely on bounding the order of the unit group rather than its structure.

For technical reasons, the main result of the paper, Theorem 3, is given in two versions. There is a bound on $|E_S/E_R|$ that holds un-

Received by the editors on June 25, 1994, and in revised form on January 28, 1995.
AMS *Mathematics Subject Classification.* 11R27.

conditionally, and a better bound that holds under special hypotheses. Just what these are will be explained later; for now, let it be noted simply that the better result applies, among other situations, if $[K : Q] \leq 8$ or if R has a power basis. In these cases,

$$|E_S/E_R| < \frac{|S/R|^2}{p-1}.$$

The general version involves a higher power of the ring index.

2. We assume from now on that S/R is a p-group. In this section we decompose S/R into a sequence of extensions of a simple type.

Lemma 1. *There are intermediate rings* $R = R_0 \subset R_1 \subset \cdots \subset R_m = S$ *such that each extension* R_{i+1}/R_i *has the additive structure* $Z_p \oplus \cdots \oplus Z_p$ *some number of times.*

Proof. Suppose that

$$R = Z[\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t],$$

and

$$S = Z\left[\alpha_1, \dots, \alpha_s, \frac{\beta_1}{p^{c_1}}, \cdots, \frac{\beta_t}{p^{c_t}}\right],$$

with $1 \leq c_1 \leq \cdots \leq c_t$. With $S = R_m$, define R_{m-1} by

$$R_{m-1} = Z\left[\alpha_1, \dots, \alpha_s, \frac{p\beta_1}{p^{c_1}}, \dots, \frac{p\beta_t}{p^{c_t}}\right];$$

that is, each basis element of S with a denominator is multiplied by p. As presented, R_{m-1} clearly is an additive group. Further, it is multiplicatively closed, because

$$\alpha_i \cdot \alpha_j \in R \subset R_{m-1}$$
$$\alpha_i \cdot \frac{p\beta_j}{p^{c_j}} \in pS \subset R_{m-1}$$
$$\frac{p\beta_i}{p^{c_i}} \cdot \frac{p\beta_j}{p^{c_j}} \in pS \subset R_{m-1}.$$

One constructs R_{m-2} from R_{m-1} in the same manner: each basis element of R_{m-1} which still has a denominator is multiplied by p. After c_t steps of this type one comes down to R. $\square$

Lemma 2. *With the notation of Lemma* 1, *let E_i denote the unit group of R_i. For $0 \le i \le c_t - 2$, E_{i+1}/E_i has exponent* 1 *or p.*

Proof. For i in the range given, we may renotate Z-bases for R_i, R_{i+1} and R_{i+2} in the form

$$\begin{aligned} R_i &= Z[\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t] \\ R_{i+1} &= Z\left[\alpha_1, \dots, \alpha_s, \frac{\beta_1}{p}, \dots, \frac{\beta_t}{p}\right] \\ R_{i+2} &= Z\left[\frac{\alpha_1}{p^{b_1}}, \dots, \frac{\alpha_s}{p^{b_s}}, \frac{\beta_1}{p^2}, \dots, \frac{\beta_t}{p^2}\right], \end{aligned}$$

where each $b_j = 0$ or 1. Let $\varepsilon \in R_{i+1}$; we show that $\varepsilon^p \in R_i$. Let $\varepsilon = \alpha + \beta/p$, where α is a Z-linear combination of $\alpha_1, \dots, \alpha_s$ and β is a Z-linear combination of $\beta_1, \dots, \beta_t$. Then

$$\varepsilon^p = \sum_{j=0}^{p} \binom{p}{j} \alpha^{p-j} p^j \left(\frac{\beta}{p^2}\right)^j.$$

Now, $(\beta/p^2)^j \in R_{i+2}$, so $p^2 \cdot (\beta/p^2)^j \in R_i$. Thus, each term in the sum with $j \ge 2$ is in R_i. Hence,

$$\varepsilon^p \equiv \alpha^p + p\alpha^{p-1}\frac{\beta}{p} \equiv 0 \bmod R_i,$$

that is, $\varepsilon^p \in R_i$. $\square$

3. In this section we focus on just one step of the chain described in Lemma 1. Let

$$R = Z[\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_r], \tag{1}$$

and

$$S = Z\left[\alpha_1, \dots, \alpha_m, \frac{\beta_1}{p}, \cdots, \frac{\beta_r}{p}\right].$$

Each unit ε in S may be written as

$$\varepsilon = \sum_{j=1}^{r} a_j \frac{\beta_j}{p} + \sigma, \tag{2}$$

with $a_j \in Z$ and $\sigma \in R$. Multiplying σ by each β_j/p leads to a congruence of the form

$$\sigma \frac{\beta_j}{p} \equiv \sum_{i=1}^{r} b_{ij} \frac{\beta_i}{p} \bmod R,$$

where the coefficients b_{ij} may be taken $\bmod p$. If we set $B = [b_{ij}]$, we have a map

$$\rho : R \longrightarrow M_r(F_p)$$

defined by $\rho(\sigma) = B$.

Another way to look at ρ is to consider for $\sigma \in R$ the linear map from S to S defined by multiplication by σ. With respect to the basis for S in (1), this map has the matrix

$$A_\sigma = \begin{array}{c c} & \begin{array}{cc} m & r \end{array} \\ \begin{array}{c} m \\ r \end{array} & \begin{pmatrix} * & * \\ pC_\sigma & B_\sigma \end{pmatrix} \end{array}$$

where B_σ and C_σ have integral entries. The lower left block is divisible by p because $\sigma\alpha_j \in R$, so involves $p \cdot (\beta_i/p)$ for each i. Composing two such maps for σ and $\tau \in R$, we see that $A_{\sigma\tau} = A_\sigma A_\tau$, so $B_{\sigma\tau} \equiv B_\sigma B_\tau \bmod p$. Hence $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$. Since ρ clearly is additive, ρ is a ring homomorphism from R into $M_r(F_p)$. If we set $W = \operatorname{Im} \rho$, W is a commutative algebra inside $M_r(F_p)$. It will be important to bound the dimension of W. In general, this can be as large as $1 + [r^2/4]$ by a theorem of Schur [**1**, p. 95]. However, $\dim W \leq r$ in several special cases to be described presently.

Referring to the form of ε in (2), σ is not unique. However, changing the coefficients $a_j \bmod p$ will change σ by an element of pS and $pS \subset \operatorname{Ker} \rho$. Thus $\rho(\sigma)$ is well-defined in terms of ε.

Note also that W is generated by the images of $\alpha_1, \dots, \alpha_m$ only, since each $\beta_i \in \operatorname{Ker} \rho$.

Lemma 3. *In* (1)*, let* $\alpha_1, \dots, \alpha_m$ *be polynomials in* α *with integral coefficients for some* $\alpha \in R$. *Then* $\dim W \leq r$.

Proof. If $B = \rho(\alpha)$, then $B^k = \rho(\alpha^k)$, so W is contained in the span of $I, B, B^2, ...$, which has dimension $\leq r$. □

In what follows, we will use an algebraic extension F of F_p in which the eigenvalues of a certain matrix lie, so that the matrix may be taken in Jordan form. For $W \leq M_r(F_p)$, $\dim W$ is the same whether computed in F_p or extending the base field to F.

Lemma 4. *Let* $J, X \in M_r(F)$ *where* $JX = XJ$ *and* J *is in Jordan form. Let* $V = \operatorname{span}\{J^i, J^i X \mid i \geq 0\}$. *Then* $\dim V \leq r$.

Proof. Write J in the form $J = J_1 \oplus \cdots \oplus J_t$, where each J_i in turn is a direct sum of Jordan blocks corresponding to the eigenvalue λ_i and $\lambda_1, \dots, \lambda_t$ are distinct. Let k_i and l_i be the sizes of the largest and next largest Jordan blocks in J_i. Take $l_i = 0$ if J_i is just one Jordan block. The degree of the minimal polynomial of J is $k = k_1 + \cdots + k_t$, as $(J_i - \lambda_i I)^{k_i} = O$ for each i. Since X commutes with J, by Lemma 4, [**1**, p. 25], X splits as a direct sum $X = X_1 \oplus \cdots \oplus X_t$, where each X_i has the same size as J_i. Further, X_i and J_i must commute, and this implies that each X_i is blocked out into triangularly striped matrices whose sizes are given by the sizes of the Jordan blocks which comprise J_i, by Theorem 6 [**1**, p. 28]. Now $(J_i - \lambda_i I)^{l_i}$ is O if $l_i = k_i$ and involves only the largest Jordan block of J_i if $l_i < k_i$. Consequently, $(J_i - \lambda_i I)^{l_i} X_i$ has nonzero entries only in the block corresponding to the largest Jordan block of J_i, and these nonzero entries are pushed l_i spaces toward the upper right corner of that block. A suitable linear combination of the matrices $(J_i - \lambda_i I)^t$, where $t \geq l_i$, will match this exactly. Thus $(J_i - \lambda_i I)^{l_i} X_i$ is a polynomial in J_i for each i. Let

$$f(x) = \prod_{i=1}^{t} (x - \lambda_i)^{l_i},$$

of degree $l = l_1 + \cdots + l_t$, and let $J' = f(J)$. Then $J'X$ is a polynomial in J, so V is spanned by

$$I, J, \dots, J^{k-1}, X, JX, \dots, J^{l-1}X,$$

and $\dim V \leq k+l \leq r$. □

Lemma 5. *In (1), let $\alpha_1, \dots, \alpha_k$ be polynomials in α, and let $\alpha_{k+1}, \dots, \alpha_m$ be monic polynomials in α divided by p^d with the same d for each term, where all the polynomials have integral coefficients and distinct degrees and $\alpha \in R$. Then* $\dim W \leq r$.

Proof. Let $B = \rho(\alpha)$, and let $C = \rho(\gamma)$ where $\gamma = \alpha_j$ with minimal degree having p^d in the denominator. Over a suitable field F, B and C are similar to J and X, respectively, as in Lemma 4. The algebra W is contained in span $\{B^i, B^iC\}$, and this is conjugate to span $\{J^i, J^iX\}$ in $M_r(F)$. Hence $\dim W \leq r$. □

In attempting to extend Lemma 5 to a situation where R has a more complicated Z-basis, one is led to a problem like that discussed in Lemma 4, but with three or more matrices. The present method breaks down at this point because examples exist of matrices J, X and $Y \in M_r(F_p)$ which commute with each other, and $\dim \operatorname{span} \{J^i, J^iX, J^iY\} > r$.

Theorem 1. *Let $S/R \simeq Z_p^r$ for some r, and let* $\dim W = d$. *Then*

$$|E_S/E_R| \leq \frac{p^{r+d}-1}{p-1}.$$

Proof. Let W be generated by $A_1, \dots, A_d$. For $\varepsilon \in E_S$, write ε as in (2),

$$\varepsilon = \sum_{j=1}^{r} a_j \frac{\beta_j}{p} + \sigma,$$

where

$$\rho(\sigma) = \sum_{j=1}^{d} s_j A_j.$$

As was noted previously, $\rho(\sigma)$ is well-defined in terms of ε, so ε leads to a point $P(\varepsilon) = (a_1, \dots, a_r, s_1, \dots, s_d)$ over F_p. If $\varepsilon \notin R$, some $a_j \neq 0$, and if $\varepsilon \in R$, then $\rho(\varepsilon\varepsilon^{-1}) = \rho(1) = I$, so some $s_j \neq 0$. Thus, we may view $P(\varepsilon)$ as a projective point over F_p. In this way we have a function P from E_S to $(r+d-1)$-dimensional projective space over F_p. We claim that if η and $\eta' \in E_S$ such that $P(\eta) = P(\eta')$, then $\eta \sim \eta'$ in the group E_S/E_R. This clearly implies that the order of E_S/E_R is bounded by the number of projective points, which is $(p^{r+d}-1)/(p-1)$. To verify the claim, suppose that

$$\eta = \sum_{j=1}^{r} b_j \frac{\beta_j}{p} + \tau,$$

and $P(\eta) = (b_1, \ldots, b_r, t_1, \ldots, t_d)$. Then

$$\varepsilon\eta \equiv \sum_{j=1}^{r} c_j \frac{\beta_j}{p} \bmod R$$

for numbers $c_1, \ldots, c_r \bmod p$ that can be computed as follows: let

$$\frac{\beta_i\beta_j}{p^2} \equiv \sum_{k=1}^{r} x_{ijk} \frac{\beta_k}{p} \bmod R.$$

Then

$$\varepsilon\eta = \sigma\tau + \sum_{j=1}^{r} b_j \left(\sigma\frac{\beta_j}{p}\right) + \sum_{j=1}^{r} a_j \left(\tau\frac{\beta_j}{p}\right) + \sum_{i=1}^{r}\sum_{j=1}^{r} a_i b_j \frac{\beta_i\beta_j}{p^2}.$$

Since $\sigma\tau \in R$, the cs are given $\bmod p$ by

$$\begin{bmatrix} c_1 \\ \vdots \\ c_r \end{bmatrix} = \sum_{i=1}^{d} s_i A_i \begin{bmatrix} b_1 \\ \vdots \\ b_r \end{bmatrix} + \sum_{i=1}^{d} t_i A_i \begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} + \begin{bmatrix} \vdots \\ \sum_{i,j} a_i b_j x_{ijk} \\ \vdots \end{bmatrix}.$$

Here the A_i and x_{ijk} are constants. The significant fact to note about the formula for $c_1, \ldots, c_r$ is that it is unaffected, projectively, if the coefficients $(b_1, \ldots, b_r, t_1, \ldots, t_d)$ are multiplied by a nonzero constant mod p. So if $P(\eta) = P(\eta')$, then $\varepsilon\eta \equiv h\varepsilon\eta' \bmod R$ for an integer h such that $p \nmid h$. This holds for every ε in E_S (with h depending on ε). In particular, let $\varepsilon = \eta^{-1}$. Then $\eta'\eta^{-1} \in R$, which is to say that $\eta \sim \eta'$ in E_S/E_R, as the claim asserted. $\square$

When $r = 1$ in Theorem 1, E_S/E_R is cyclic, as shown in [**2**]. When $r > 1$, however, noncyclic cases may occur. For example, in the field $Q(\alpha)$, where $\alpha^3 = 3\alpha - 1$, let $S = Z[\alpha]$ and $R = Z[1, 3\alpha, 3\alpha^2]$. S has fundamental units α and $\alpha^2 + \alpha - 2$, while R has their cubes as fundamental units. Hence, $E_S/E_R \simeq C_3 \times C_3$.

4. Let R and S be as in Lemma 1:

$$\begin{aligned} R &= Z[\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t] \\ S &= Z\left[\alpha_1, \dots, \alpha_s, \frac{\beta_1}{p^{c_1}}, \cdots, \frac{\beta_t}{p^{c_t}}\right] \end{aligned} \tag{3}$$

with $1 \leq c_1 \leq \cdots \leq c_t$. There is a chain of rings, as described in Lemma 1, of the form

$$R = R_0 \subset R_1 \subset \cdots \subset R_{m-1} \subset R_m = S. \tag{4}$$

Here $m = c_t$. Each extension $R_{i+1}/R_i \simeq Z_p^{r_i}$ for some r_i, as additive groups. As in Section 3, this leads to an algebra $W_i \leq M_{r_i}(F_p)$. The following theorem lists several natural situations in which $\dim W_i \leq r_i$ at each step of the chain in (4).

Theorem 2. *In the notation just established,* $\dim W_i \leq r_i$ *for each* i *if any of the following hold*:

1. $[K : Q] \leq 8$.
2. S/R *has* ≤ 3 *generators.*
3. $R = Z[\alpha]$ *for some* α.
4. R *has a* Z*-basis* $1, \alpha, \dots, \alpha^{k-1}, f_k(\alpha)/p^d, \dots, f_{n-1}(\alpha)/p^d$ *with each* f_j *monic over* Z*, with degree* j*.*

Proof. 1. Only when $r \geq 4$ is it possible to have $\dim W > r$. Further, in the construction of W in Section 3, W is generated by m elements, where m is the number of basis elements common to the two rings. To have $\dim W > r$ requires $m > r$ obviously. Hence there must be at least nine elements in a basis.

2. When $r < 4$, $1 + [r^2/4] = r$.

3. When R has a power basis, the common part of the bases for R_i and R_{i+1} consists of the first so many powers of α. Hence, Lemma 3 applies at each step.

4. As in part 3, using Lemma 5. □

Theorem 3. *Let $S/R \simeq Z_{p^{c_1}} \oplus \cdots \oplus Z_{p^{c_t}}$ with $1 \leq c_1 \leq \cdots \leq c_t$, and let $C = c_1 + \cdots + c_t$. Then*

$$|E_S/E_R| < \frac{p}{p-1} \cdot p^{C(1+t/4)}.$$

If $\dim W_i \leq r_i$ at each step of (4), *then*

$$|E_S/E_R| < \frac{p}{p-1} \cdot p^{2C-c_t} \leq \frac{|S/R|^2}{p-1}.$$

Proof. Keeping the notation of (3) and (4), each $R_{i+1}/R_i \simeq Z_p^{r_i}$ for some r_i. The number of extensions of each type is as follows:

$$\begin{cases} c_1 & \text{have type } Z_p^t \\ c_2 - c_1 & \text{have type } Z_p^{t-1} \\ \vdots & \\ c_t - c_{t-1} & \text{have type } Z_p \end{cases}$$

The total number is c_t, the number of steps from R to S. For all but the last step, E_{i+1}/E_i is a p-group by Lemma 2. So the bound in Theorem 1 can be sharpened slightly, to p^{r+d-1}, except for the last step. First, assume $\dim W_i \leq r_i$ at each step, so $d \leq r_i$ in Theorem 1. Then

$$\begin{aligned} |E_S/E_R| &\leq p^{c_t - c_{t-1}} \cdot p^{3(c_{t-1}-c_{t-2})} \cdots p^{(2t-1)(c_1-1)} \cdot \frac{p^{2t}-1}{p-1} \\ &= p^{c_t + 2(c_1 + \cdots + c_{t-1})} \cdot p^{1-2t} \cdot \frac{p^{2t}-1}{p-1} \\ &< \frac{p^{2C-c_t+1}}{p-1}, \end{aligned}$$

as stated in the theorem. Note that $|S/R| = p^C$.

Next consider the general case, where we may say only that $d \leq 1 + [r_i^2/4]$ at each step. Then

$$|E_S/E_R| \leq \prod_{j=1}^{t} p^{(j+[j^2/4])(c_{t-j+1}-c_{t-j})} \cdot \frac{p^{[t^2/4]+t+1}-1}{p-1}.$$

Here $c_0 = 1$. For k odd, the coefficient of c_{t-k} in the exponent of the product is

$$-\left(k + \frac{k^2-1}{4}\right) + \left(k+1+\frac{(k+1)^2}{4}\right) = \frac{k+3}{2}.$$

For k even, the coefficient is $(k+2)/2 = ((k-1)+3)/2$. So the total exponent of the product is

$$(5) \quad (c_t + 2(c_{t-1}+c_{t-2}) + 3(c_{t-3}+c_{t-4}) + 4(c_{t-5}+c_{t-6}) + \cdots) \\ - (t + [t^2/4]).$$

The last term comes from the c_0 coefficient. Since the c_j are increasing,

$$c_1 + \cdots c_k \leq \frac{kC}{t}.$$

The sum in parentheses at (5) is, for t even,

$$\begin{aligned} &c_t + 2(c_{t-1}+c_{t-2}) + \cdots + \frac{t}{2}(c_3+c_2) + \frac{t+2}{2}c_1 \\ &\quad = C + (c_1 + \cdots + c_{t-1}) + (c_1 \cdots + c_{t-3}) + \cdots + (c_1 + c_3) + c_1 \\ &\quad \leq C\left(1 + \frac{t-1}{t} + \frac{t-3}{t} + \cdots + \frac{3}{t} + \frac{1}{t}\right) \\ &\quad = C(1+t/4). \end{aligned}$$

For t odd, one obtains $C(1+(t^2-1)/(4t)) < C(1+t/4)$ in the same way. This leads to the result as stated in the theorem. □

Theorem 4. *Let $K = Q(\alpha)$ where α is an algebraic integer, and suppose that $D(\alpha) = D(K/Q) \cdot p^{2m}$ for some $m \geq 1$, where D denotes* *discriminant. Let $R = Z[\alpha]$ and $S = O_K$, the full ring of integers in K. Then*

$$|E_S/E_R| < \frac{p^{2m}}{p-1}.$$

Proof. When $R = Z[\alpha]$, $\dim W_i \leq r_i$ at each step, by Theorem 2. The result follows from Theorem 3; note that $C = m$ here. □

By piecing together Theorem 4 for each prime factor of the ring index, we obtain the final result:

Corollary. *Let K, R and S be as in Theorem* 4*, except that*

$$\frac{D(\alpha)}{D(K/Q)} = \prod_{j=1}^{s} p_j^{2m_j}$$

with distinct p_j and each $m_j \geq 1$. Then

$$|E_S/E_R| < \prod_{j=1}^{s} \frac{p_j^{2m_j}}{p_j - 1}.$$

REFERENCES

1. Suprunenko and Tyshkevich, *Commutative matrices*, Academic Press, New York, 1968.

2. J. Wolfskill, *Bounding a unit index in terms of a ring index*, Mathematika **42** (1995), 199–205.

Department of Mathematics, Northern Illinois University, DeKalb, Illinois 60115
E-mail address: wolfskil@math.niu.edu