Tôhoku Math. J.
46 (1994), 141–145

ON SILVERMAN'S ESTIMATE OF REGULATORS

KÔJI UCHIDA

(Received September 10, 1992, revised March 26, 1993)

Abstract. Silverman proved that the size of the regulator of the algebraic number field grows at least with some power of the logarithm of the absolute value of the dicriminant, multiplied by some constant depending only on the degree of the field. He also stated that the exponent he obtained may be the best. But it is not the best in many cases and we can replace it by better one.

Let K be an algebraic number field of degree $n \geqq 2$. Let D_K and R_K be the discriminant and the regulator of K, respectively. Let r be the rank of the unit group of K, and ρ be the maximum of the ranks of the unit groups of proper subfields of K. Silverman [5] proved an inequality

$$R_K > c_n(\log d_n |D_K|)^{r-\rho}$$

for some positive constants c_n and d_n depending only on the degree n. Friedman [2] improved the estimate of constants c_n and d_n, and especially he proved that d_n can be n^{-n}. It should be noted that the above inequality is valid only when $\log(d_n|D_K|) > 0$. Silverman stated that the exponent $r-\rho$ will probably be best possible. However we will find a better exponent, because the following easy examples show that this exponent is not always the best.

EXAMPLE. Let K be $Q(\sqrt{-3}, \sqrt[3]{m})$, $Q(\sqrt[4]{m})$ or $Q(\sqrt{-a}, \sqrt{m})$ for a fixed positive integer a. If m is a positive integer, the subfield with unit rank ρ is $Q(\sqrt[3]{m})$ or $Q(\sqrt{m})$. When m moves over square free positive integers, the discriminant of this subfield also grows with m. Hence the exponent should be r instead of $r-\rho$ in this case.

Let c be a constant greater than 1. Let F be a maximal subfield of K satisfying the inequality

$$(*) \qquad |D_F| < |D_K|^{1/[K:F]^c}.$$

We can find such an F in every case, because the rational number field Q satisfies this inequality while K does not. Then we can prove the following:

1991 *Mathematics Subject Classification*. Primary 11R27.

Partly supported by the Grants-in-Aid for Scientific Research, The Ministry of Education, Science and Culture, Japan.

THEOREM. *Let K be an algebraic number field of degree $n \geqq 2$. Let D_K and R_K be the discriminant and the regulator of K, respectively. Let r be the rank of the unit group of K, and let λ be the rank of the unit group of F. Then R_K satisfies an inequality*

$$R_K > c_n(\log d_n |D_K|)^{r-\lambda}$$

for some positive constants c_n and d_n depending only on the degree n, if $d_n|D_K|>1$.

We first prove some lemmas.

LEMMA 1. *Let α be an element of K which is not contained in F, and let $m = [F(\alpha):F]$. Then the absolute norm of the relative discriminant $D_{F(\alpha)/F}$ satisfies*

$$N_F(D_{F(\alpha)/F}) \geqq |D_K|^{(m^c-m)/[K:F]^c}\,.$$

PROOF. Since $|D_{F(\alpha)}| = |D_F|^m \cdot N_F(D_{F(\alpha)/F})$ and since $D_{F(\alpha)}$ does not satisfy the inequality $(*)$, we have

$$\begin{aligned} |D_K|^{1/[K:F(\alpha)]^c} &\leqq |D_{F(\alpha)}| = |D_F|^m \cdot N_F(D_{F(\alpha)/F}) \\ &\leqq |D_K|^{m/[K:F]^c} \cdot N_F(D_{F(\alpha)/F})\,. \end{aligned}$$

Let F, α and m be as above and let us also assume that α is an algebraic integer. Then the relative discriminant of α

$$\Delta(\alpha) = \begin{vmatrix} 1 & \cdots & 1 \\ \alpha^{(1)} & \cdots & \alpha^{(m)} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ (\alpha^{(1)})^{m-1} & \cdots & (\alpha^{(m)})^{m-1} \end{vmatrix}^2 .$$

generates a multiple ideal of the relative discriminant $D_{F(\alpha)/F}$, where $\alpha^{(i)}$ are the conjugates of α over F. Hadamard's inequality shows

$$|\Delta(\alpha)| \leqq \prod_{i=1}^{m} (1 + |\alpha^{(i)}|^2 + \cdots + |\alpha^{(i)}|^{2(m-1)})\,,$$

and the same inequality for every conjugate of $F(\alpha)$ over $\boldsymbol{Q}$. This leads to:

LEMMA 2.

$$N_F(D_{F(\alpha)/F}) \leqq m^{[F(\alpha):\boldsymbol{Q}]} \cdot H_{F(\alpha)}(\alpha)^{2(m-1)}\,.$$

In the above, $H_{F(\alpha)}(\alpha) = \prod \mathrm{Max}(1, |\alpha^{(i)}|)$ is the height of α, where the product is over all conjugates of $F(\alpha)$ over $\boldsymbol{Q}$.

PROOF. Since $N_F(\Delta(\alpha))$ is a multiple ideal of $N_F(D_{F(\alpha)/F})$, this is a direct consequence of the above inequalities and

$$1+|\alpha^{(i)}|^2+\cdots+|\alpha^{(i)}|^{2(m-1)}\leqq m\cdot \mathrm{Max}(1, |\alpha^{(i)}|^{2(m-1)}).$$

Remark. This lemma is a relative case of Silverman's Proposition. Remak [4] and Friedman [2] obtained a better inequality. We adopted Silverman's simpler method. This method derives better estimate in the CM-field case.

Lemma 3. *If $F(\alpha)$ is contained in a* CM*-field and if α is not a root of unity,*

$$N_F(D_{F(\alpha)/F})\leqq H_{F(\alpha)}(\alpha)^{2m}.$$

Proof. Since $F(\alpha)$ is contained in a CM-field, $|\alpha^{(i)}|^2$ is a conjugate of $|\alpha|^2$ for every conjugate $\alpha^{(i)}$ of α over $\boldsymbol{Q}$. Taking the norm of

$$1+|\alpha^{(i)}|^2+\cdots+|\alpha^{(i)}|^{2(m-1)}=\frac{1-|\alpha^{(i)}|^{2m}}{1-|\alpha^{(i)}|^2},$$

we obtain the desired inequality, because $\prod(1-|\alpha^{(i)}|^2)$ is a non-zero rational integer and

$$\left|\prod(1-|\alpha^{(i)}|^{2m})\right|\leqq\prod \mathrm{Max}(1, |\alpha^{(i)}|^{2m})=H_{F(\alpha)}(\alpha)^{2m}.$$

We can now prove our theorem. We may suppose $r>0$. As in Friedman [2], Minkowski's theory of successive minima gives

$$R_K\geqq(r+1)^{-1/2}\gamma_r^{-r/2}\cdot\prod_{i=1}^{r} m(\varepsilon_i),$$

where γ_r is the Hermite constant, $\varepsilon_1, \ldots, \varepsilon_r$ are some independent units, and

$$m(\varepsilon_i)=\left(\sum_{j=1}^{r+1}(\log\|\varepsilon_i\|_{v_j})^2\right)^{1/2},$$

where the sum is taken over the infinite primes of K. It should be noted that $m(\varepsilon_i)$ and $L(\varepsilon_i)$ in [5] are slightly different. We follows Silverman's argument [5, p. 439], and get

$$m(\varepsilon_i)\geqq(1/\sqrt{r+1})\cdot\sum_{j=1}^{r+1}|\log\|\varepsilon_i\|_{v_j}|=(2n/\sqrt{r+1})\cdot h(\varepsilon_i),$$

where $h(\varepsilon_i)$ is the absolute logarithmic height of ε_i. We see that

$$\sqrt{r+1}\cdot\gamma_r^{r/2}\leqq\sqrt{r+1}\cdot(2/\pi)^{r/2}\Gamma(2+r/2)\leqq(r+1)^{r/2}$$

for $r\geqq 4$ and $\sqrt{r+1}\cdot\gamma_r^{r/2}\leqq(r+1)^{r/2}$ for $r\leqq 3$ by direct computation. Hence

$$\begin{aligned}R_K&\geqq(r+1)^{-1/2}\gamma_r^{-r/2}\cdot\prod_{i=1}^{r} m(\varepsilon_i)\\&\geqq(r+1)^{-r/2}\cdot\prod(2n/\sqrt{r+1})\cdot h(\varepsilon_i)\cdot\prod m(\varepsilon_i).\end{aligned}$$

In the above, the first product is taken over ε_i not in F while the second product is over ε_i in F. The number of the second ε_i's is at most λ. Dobrowolsky's theorem [1] shows that the second product is greater than a constant depending only on n. For the first product, Lemmas 1 and 2 show

$$\begin{aligned}h(\varepsilon_i) &\geqq \frac{1}{2(m-1)[F(\varepsilon_i):Q]}\log N_F(D_{F(\varepsilon_i)/F}) - \frac{\log m}{2(m-1)}\\ &\geqq \frac{m^c-m}{2(m-1)[F(\varepsilon_i):Q][K:F]^c}\log|D_K| - \frac{\log m}{2(m-1)}\\ &= \frac{(m^{c-1}-1)[F:Q]^{c-1}}{2(m-1)n^c}\log|D_K| - \frac{\log m}{2(m-1)}\,.\end{aligned}$$

Since $m^{c-1}-1=e^{(c-1)\log m}-1\geqq(c-1)\log m$, and since $(\log m)/(m-1)\geqq(\log n)/(n-1)$, we get

$$h(\varepsilon_i)\geqq\frac{\log m}{2(m-1)}\left(\frac{c-1}{n^c}\log|D_K|-1\right)\geqq\frac{(c-1)\log n}{2(n-1)n^c}\log(|D_K|/e^{n^c/(c-1)})\,.$$

This concludes the proof of our theorem and d_n can be $e^{-n^c/(c-1)}$.

REMARK. We see that $n^c/(c-1)$ is smallest when $c=1+1/\log n$. Then $n^c=en$ and we get $d_n=n^{-en}$. This value of c gives the correct exponents for large m in the above examples.

REMARK. For a subfield of a CM-field, Lemma 3 gives a better estimate

$$h(\varepsilon_i)\geqq\frac{(c-1)\log m}{2m\cdot n^c}\log|D_K|\,,$$

which gives an estimate of R_K which is valid even in the case $|D_K|<n^{en}$. However in the case $|D_K|<n^{en}$, for example, in the cyclotomic field case, the estimate is worse than the estimate given by Pohst [3].

We finally give a simple proof for Pohst's Lemma [3, p. 98].

LEMMA 4. *Let* $a_1,\dots,a_l$ *be real numbers greater than* 1. *Let* $b_1,\dots,b_m$ *be positive real numbers smaller than* 1. *We assume that*

$$A=a_1\cdots a_l=(b_1\cdots b_m)^{-1}$$

and

$$\prod_{i=1}^{l}(a_i-1)\cdot\prod_{j=1}^{m}(1-b_j)\geqq 1\,.$$

Then A *satisfies an inequality*

$$A \geqq \left(\frac{1+\sqrt{5}}{2}\right)^{l+m}.$$

PROOF. If $c_1, \dots, c_n$ are positive numbers smaller than 1, the inequality between arithmetic mean and geometric mean shows

$$(1-c_1)\cdots(1-c_n) \leqq \left(1-\frac{c_1+\cdots+c_n}{n}\right)^n \leqq (1-\sqrt[n]{c_1\cdots c_n})^n .$$

Then our assumption shows

$$\begin{aligned}1 &\leqq A\cdot\prod(1-a_i^{-1})\cdot\prod(1-b_j) \leqq A(1-\sqrt[n]{b_1\cdots b_m/a_1\cdots a_l})^n \\ &=(\sqrt[n]{A}-\sqrt[n]{A}^{-1})^n ,\end{aligned}$$

where $n=l+m$. If we put $x=\sqrt[n]{A}$, then x satisfies an inequality

$$x-x^{-1} \geqq 1 .$$

Since $x>0$, this shows $x \geqq (1+\sqrt{5})/2$ and the desired inequality.

Let ε be a unit which is not a root of unity and let m be the degree of $E=\boldsymbol{Q}(\varepsilon)$. Let $\varepsilon_1, \dots, \varepsilon_m$ be the conjugates of ε. If E is totally real or is a CM-field, we can show

$$H_E(\varepsilon) \geqq \left(\frac{1+\sqrt{5}}{2}\right)^{m/2}$$

by the above lemma because $|\prod(|\varepsilon_i|^2-1)| = |N_E(\varepsilon\bar{\varepsilon}-1)| \geqq 1$. Then

$$m_E(\varepsilon) \geqq 2\sqrt{r_E+1}^{-1}\cdot\log H_E(\varepsilon) \geqq \sqrt{m}\cdot\log\left(\frac{1+\sqrt{5}}{2}\right),$$

which is Pohst's lemma. When E is a CM-filed, $\sqrt{m}$ can be replaced by $\sqrt{2m}$.

REFERENCES

[1] E. DOBROWOLSKI, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. 34 (1979), 391–401.

[2] E. FRIEDMAN, Analytic formulas for the regulator of a number field, Invent. Math. 98 (1989), 599–622.

[3] M. POHST, Eine Regulatorabschätzung, Abh. Math. Sem. Univ. Hamburg 47 (1978), 95–106.

[4] R. REMAK, Über Grössenbeziehungen zwischen Diskriminanten und Regulator eines algebraischen Zahlkörpers, Compositio Math. 10 (1952), 245–285.

[5] J. SILVERMAN, An inequality relating the regulator and the discriminant of a number field, J. Number Theory 19 (1984), 437–442.

GRADUATE SCHOOL OF INFORMATION SCIENCE
TÔHOKU UNIVERSITY
KAWAUCHI, AOBAKU, SENDAI 980-77
JAPAN