83. The Set of Primes Bounded by the Minkowski Constant of a Number Field

By Makoto ISHIBASHI*)

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1990)

Let k be an algebraic number field with degree $m=r_1+2r_2\geqq 2$ and discriminant d_k, where (r_1, r_2) denotes the signature of k. Write $M_k=(4/\pi)^{r_2}(m!/m^m)\sqrt{|d_k|}$ (the Minkowski constant of k) and $M(k)=\{p$; rational prime and $p\leqq M_k\}$. For every prime number p, let $p\,O_k=P_1^{e_1}\cdots P_g^{e_g}$ be the decomposition into prime ideals of O_k (where O_k denotes the ring of integers in k, $P_i\neq P_j$ $(i\neq j)$ are distinct prime ideals of O_k). In general, the prime number p is not necessarily irreducible element in O_k. Let $\mathrm{Irr}(O_k)$ be the set of all irreducible elements in O_k. Now we define nine subsets $A_0(k), A_1(k), \cdots, A_8(k)$ of $M(k)$ as follows.

$A_0(k)=\{p\in M(k)$; $g=e_1=1$ (i.e. p remains prime in O_k, so) $p\in\mathrm{Irr}(O_k)\}$

$A_1(k)=\{p\in M(k)$; $g=1$, $e_1=m$ (i.e. p is fully ramified), $p\in\mathrm{Irr}(O_k)\}$

$A_2(k)=\{p\in M(k)$; $e_1+\cdots+e_g\lneqq m$, $1\lneqq e_j$ for some j, $p\in\mathrm{Irr}(O_k)\}$

$A_3(k)=\{p\in M(k)$; $g=m$, $e_1=\cdots=e_g=1$ (i.e. p splits completely), $p\in\mathrm{Irr}(O_k)\}$

$A_4(k)=\{p\in M(k)$; $g\lneqq m$, $e_1=\cdots=e_g=1$ (i.e. p is unramified), $p\in\mathrm{Irr}(O_k)\}$

$A_5(k)=\{p\in M(k)$; $g=1$, $e_1=m$ (i.e. p is fully ramified), $p\notin\mathrm{Irr}(O_k)\}$

$A_6(k)=\{p\in M(k)$; $e_1+\cdots+e_g\lneqq m$, $1\lneqq e_j$ for some j, $p\notin\mathrm{Irr}(O_k)\}$

$A_7(k)=\{p\in M(k)$; $g=m$, $e_1=\cdots=e_g=1$ (i.e. p splits completely), $p\notin\mathrm{Irr}(O_k)\}$

$A_8(k)=\{p\in M(k)$; $g\lneqq m$, $e_1=\cdots=g_g=1$ (i.e. p is unramified), $p\notin\mathrm{Irr}(O_k)\}$.

Then we have $M(k)=A_0(k)\cup A_1(k)\cup\cdots\cup A_8(k)$ (disjoint union). In case $m=2$, the subsets $A_2(k)$, $A_4(k)$, $A_6(k)$, $A_8(k)$ are of course empty.

The following three theorems are variations on the theme of T. Ono [2].

Theorem 1. *If $M(k)=A_0(k)$, then the class number h_k of k is one.*

Proof. By the Minkowski lemma, the ideal class group H_k of k is generated by the classes of prime ideals over $p\in M(k)$. Hence we have $h_k=1$. Q.E.D.

Lemma 1. *Let $aO_k=Q_1\cdots Q_n$ be the decomposition into prime ideals ($Q_1, \cdots, Q_n$ are not necessarily distinct, $a\in O_k$). Suppose that Q_i belongs to an ideal class $x_i\in H_k$ $(1\leqq i\leqq n)$ and x_0 denotes the principal class of H_k. Then a is an irreducible element in O_k if and only if $x_{i_1}\cdots x_{i_m}\neq x_0$ for every proper subset $\{i_1, \cdots, i_m\}$ of $\{1, \cdots, n\}$.*

Proof. See Lemma 1.2 in Czogala [1]. Q.E.D.

Theorem 2. *If $\sharp(A_1(k)\cup A_3(k))\geqq 1$, then $h_k\geqq m=(k:Q)$.*

*) 1-27-10 Kitahara-cho, Tanashi-shi, Tokyo 188.

Proof. Assume that $p \in M(k) \cap \mathrm{Irr}(O_k)$ and $pO_k = P_1^{e_1} \cdots P_g^{e_g}$. By Lemma 1, the ideals $P_1, P_1^2, \cdots, P_1^{e_1}, P_1^{e_1}P_2, \cdots, P_1^{e_1}P_2^{e_2}, \cdots, P_1^{e_1}P_2^{e_2} \cdots P_{g-1}^{e_{g-1}}P_g, \cdots, P_1^{e_1}P_2^{e_2} \cdots P_{g-1}^{e_{g-1}}P_g^{e_g}$ are non-equivalent. Hence we have $e_1 + \cdots + e_g \leqq h_k$. Therefore, $p \in A_1(k) \cup A_3(k)$ implies $e_1 + \cdots + e_g = m$. This completes our proof.

Q.E.D.

Theorem 3. *Let V_m be the family of all algebraic number fields k with a fixed degree m and $M_k \geqq 3$. For each $k \in V_m$, write $d_k = (-1)^{r_2} p_{p_1}^{e_1} \cdots p_{s(k)}^{e_{s(k)}} p_{s(k)+b_1}^{f_1} \cdots p_{s(k)+b_{t(k)}}^{f_{t(k)}}$, where p_j denotes j-th rational prime ($j = 1, 2, \cdots$) and $p_{s(k)} \leqq M_k < p_{s(k)+1}$ ($b_1 < \cdots < b_{t(k)}$). Suppose that $W_m = \{k \in V_m ; e_{s(k)-1} \geqq 1$ and $e_{s(k)} \geqq 1\}$. Then W_m is a finite set.*

Proof. From Tschebysheff's theorem (i.e. $p_{j+1} < 2p_j$) and $p_s + 2b \leqq p_{s+b}$ ($b \geqq 1, s \geqq 2$), it follows that

$$(m!/m^m)^2 p_1^{e_1} \cdots p_{s(k)}^{e_{s(k)}} (p_{s(k)} + 2b_1)^{f_1} \cdots (p_{s(k)} + 2b_{t(k)})^{f_{t(k)}} < 4p_{s(k)}^2.$$

Hence we have

$$p_1^{e_1} \cdots p_{s(k)-2}^{e_{s(k)-2}} p_{s(k)-1}^{e_{s(k)-1}-1} p_{s(k)}^{e_{s(k)}-1} (p_{s(k)} + 2b_1)^{f_1} \cdots (p_{s(k)} + 2b_{t(k)})^{f_{t(k)}} < 8m^{2m}/(m!)^2.$$

Thus $s(k)$, $t(k)$, e_j ($1 \leqq j \leqq s(k)$), f_j ($1 \leqq j \leqq t(k)$), $b_1, \cdots, b_{t(k)}$ are bounded. Therefore, the absolute values of d_k ($k \in W_m$) are bounded from above by a positive constant (independent of k, and only dependent on m). Since there exist only finitely many number fields with a fixed given discriminant, we know that W_m is a finite set. Q.E.D.

References

[1] Czogala, A.: Arithmetical characterization of algebraic number fields with small class number. Math. Zeit., **176**, 247–253 (1981).

[2] Ono, T.: A problem on quadratic fields. Proc. Japan Acad., **64A**, 78–79 (1988).