[3] G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsber. Preuss. Akad. Wiss., Math.-Phys. Kl., Berlin 1896.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetze*, Jahresber. der Deutschen Mathematischen Vereinigung, Bd. 36, Berlin 1930.

[5] T. Nagell, *Zahlentheoretische Notizen I, Ein Beitrag zur Theorie der höheren Kongruenzen*, Videnskapsselskapets Skrifter I, Matem.-Naturv. Klasse, No. 13, Kristiania 1923.

[6] — *Introduction to number theory*, New York 1951.

[7] — *Sur quelques problèmes dans la théorie des restes quadratiques et cubiques*, Ark. Mat. 3 (16), Stockholm 1955.

[8] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berliner Math. Gesellsch., 11. Jahrg., Berlin 1912.

INSTITUT DE MATHÉMATIQUES DE L'UNIVERSITÉ D'UPPSALA

Reçu par la Rédaction le 2. 5. 1968

ACTA ARITHMETICA
XV (1969)

Remarque sur le travail précédent de T. Nagell

par

A. Schinzel (Varsovie)

Dans le travail [3] qui précède T. Nagell demande quels sont pour un nombre n donné quelconque les polynômes, dont tous les diviseurs premiers sont de la forme $nt+1$, abstraction faite d'un nombre fini des cas. Il suffit évidemment de résoudre ce problème pour les polynômes irréductibles. Nous allons démontrer

Théorème. *Soit n un nombre naturel quelconque, ζ_n une racine primitive de degré n de l'unité et soit $G(x)$ un polynôme irréductible. Afin que tous les diviseurs premiers de $G(x)$, abstraction faite d'un nombre fini des cas, soient de la forme $nt+1$ il faut et il suffit que*

$$(*) \qquad G(x) = aN\big(H(x)\big),$$

où $H(x)$ est un polynôme à coefficients du corps $Q(\zeta_n)$, N est la norme dans ce corps et a est un nombre rationnel.

Démonstration. Nécessité. Soit θ une racine de G et soit $k = Q(\theta)$ le corps engendré par θ. Les nombres premiers, qui ont un facteur premier idéal de degré 1 dans k sont des diviseurs de $G(x)$, donc étant de la forme $nt+1$ ils se décomposent complètement dans le corps $Q(\zeta_n)$. En vertu du théorème de Bauer ([1], voir [2], lemme 3) $Q(\zeta_n)$ est contenu dans k. La condition $(*)$ résulte maintenant du lemme 2 de [2] après la substitution $J = Q(\zeta_n)$.

Suffisance. Posons dans le lemme 1 de [2] $f(x) = G(x)/a$, $K = Q(\zeta_n)$. Les hypothèses étant satisfaites il en résulte que tous les diviseurs premiers suffisamment grands de $G(x)$ se décomposent dans K en facteurs premiers idéaux de degré 1. Ceci veut dire que ces diviseurs sont de la forme $nt+1$, q.e.d.

Dans le même ordre d'idées on peut démontrer le théorème plus général suivant:

Soit J un corps Bauerien (cf. [4], p. 333) *et soit $G(x)$ un polynôme irréductible. Afin que tous les diviseurs premiers de $G(x)$, abstraction faite*

d'un nombre fini des cas, aient un facteur premier idéal de degré 1 *dans* J, *il faut et il suffit que*

$$G(x) = aN\big(H(x)\big),$$

où $H(x)$ *est un polynôme à coefficients de* J, N *est la norme dans* J *et* a *est un nombre rationnel.*

La propriété des corps Baueriens éxprimée dans ce théorème est caracteristique: pour les autres corps p.ex. $Q\big(\sqrt{2\cos(2\pi/7)}\big)$ (cf. [4], p. 335) le théorème est en défaut.

Travaux cités

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), p. 353-356.

[2] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), p. 107-116.

[3] T. Nagell, *Sur les diviseurs premiers des polynômes*, Acta Arith. ce fasc., p. 235-244.

[4] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), p. 333-344. Corrigendum, ibid. 12 (1967), p. 425.

Reçu par la Rédaction le 22. 6. 1968

ACTA ARITHMETICA
XV (1969)

Gauss sums over finite fields of order 2^n *

by

L. Carlitz (Durham, North Carolina)

1. Introduction. Let $F = \mathrm{GF}(q)$ denote the finite field of order q; we shall assume throughout the paper that $q = 2^n$, $n \geqslant 1$. For $a \in F$ put

$$t(a) = a + a^2 + a^{2^2} + \ldots + a^{2^{n-1}},$$

so that $t(a) \in \mathrm{GF}(2)$. Define

$$e(a) = (-1)^{t(a)}.$$

Let

$$Q(x) = Q(x_1, \ldots, x_m) = \sum_{1 \leqslant i \leqslant j \leqslant m} a_{ij} x_i x_j \qquad (a_{ij} \in F) \tag{1.1}$$

denote a quadratic form over F. If

$$y_i = \sum_{j=1}^{m} c_{ij} x_j \qquad (c_{ij} \in F,\ |c_{ij}| \neq 0)$$

and

$$Q(x_1, \ldots, x_m) = Q_1(y_1, \ldots, y_m),$$

the quadratic forms $Q(x)$ and $Q_1(y)$ are *equivalent*. Dickson ([2], p. 197) has proved that if $Q(x)$ is not equivalent to a form in fewer than m indeterminates then it is equivalent to either

$$y_1y_2 + y_3y_4 + \ldots + y_{m-2}y_{m-1} + y_m^2 \tag{1.2}$$

when m is odd or to one of the forms

$$y_1y_2 + y_3y_4 + \ldots + y_{m-1}y_m \tag{1.3}$$

or

$$y_1y_2 + \ldots + y_{m-3}y_{m-2} + y_{m-1}^2 + y_{m-1}y_m + \beta y_m^2 \tag{1.4}$$

* Supported in part by NSF grant GP-1855.