

Über eine Aufgabe von Schur.

Von IVÁN SERES in Budapest.

I. SCHUR hat folgende Aufgabe gestellt:

Seien $a_1, a_2, \dots, a_m$ verschiedene ganze Zahlen. Man beweise, daß das Polynom

$$F(u) = \prod_{i=1}^m (u - a_i)^{2^n} + 1$$

für $n > 1$ irreduzibel ist.

Es ist mir gelungen obigen Satz für $m=2$ zu beweisen; dabei kann die Beschränkung $a_1 \neq a_2$ fallen lassen werden.

Beweis: Es sei $u - a_1 = x$. Dann geht $F(u)$ in folgendes Polynom über:

$$F(u) = G(x) = [x(x+a)]^{2^n} + 1,$$

$a = a_1 - a_2$. Nehmen wir an, daß $G(x)$ reduzibel ist:

$$G(x) = g(x)h(x),$$

wobei $g(x)$ und $h(x)$ ganzzahlige, nichtkonstante Polynome sind. Es gelten

$$G(x) \equiv g(x)h(x) \pmod{2},$$

und

$$G(x) \equiv (x^2 + ax)^{2^n} + 1 \equiv (x^2 + ax + 1)^{2^n} \pmod{2}.$$

Hieraus folgt

$$(1) \quad (x^2 + ax + 1)^{2^n} \equiv g(x)h(x) \pmod{2}.$$

Wir unterscheiden zwei Fälle:

FALL I: $2 \nmid a$.

In diesem Falle kann (1) so geschrieben werden

$$(2) \quad (x^2 + x + 1)^{2^n} \equiv g(x)h(x) \pmod{2}.$$

Da $x^2 + x + 1 \pmod{2}$ irreduzibel ist, folgt aus (2)

$$\begin{aligned} g(x) &= (x^2 + x + 1)^r + 2A(x), \quad r \geq 1, \\ h(x) &= (x^2 + x + 1)^s + 2B(x), \quad s \geq 1, \end{aligned}$$

wobei $r+s=2^n$, während $A(x)$ und $B(x)$ ganzzahlige Polynome sind. Es gilt

$$(3) \quad G(x) = (x^2 + ax)^{2^n} + 1 \equiv (x^2 + x + 1)^{s+r} + 2[(x^2 + x + 1)^s A(x) + (x^2 + x + 1)^r B(x)] \pmod{4}.$$

Mit Rücksicht auf

$$(4) \quad (x^2 + x + 1)^{2^n} \equiv (x^2 + x)^{2^n} + 2(x^2 + x)^{2^{n-1}} + 1 \pmod{4}$$

gilt wegen (3) und $2 \nmid a$:

$$G(x) \equiv (x^2 + x)^{2^n} + 1 \equiv (x^2 + x)^{2^n} + 2(x^2 + x)^{2^{n-1}} + 1 + 2[(x^2 + x + 1)^s A(x) + (x^2 + x + 1)^r B(x)] \pmod{4}.$$

Nach Division durch 2 erhält man

$$(x^2 + x)^{2^{n-1}} \equiv (x^2 + x + 1)^s A(x) + (x^2 + x + 1)^r B(x) \pmod{2}.$$

Die rechte Seite enthält den mod 2 irreduziblen Faktor $x^2 + x + 1$, während die linke Seite nicht. Dies ist wegen der Eindeutigkeit der Faktorisierung mod 2 unmöglich.

FALL II: $2|a$.

Dann folgert man aus (1):

$$G(x) \equiv (x^2 + 2x + 1)^{2^n} \equiv (x + 1)^{2^{n+1}} \pmod{2}$$

$$g(x) = (x + 1)^r + 2A(x), \quad r \geq 1,$$

$$h(x) = (x + 1)^s + 2B(x), \quad s \geq 1,$$

mit $r+s=2^{n+1}$. Offenbar gilt:

$$(5) \quad G(x) \equiv (x^2 + ax)^{2^n} + 1 \equiv x^{2^{n+1}} + 1 \pmod{4}.$$

Andererseits gilt nach (1)

$$G(x) \equiv (x + 1)^{r+s} + 2[(x + 1)^s A(x) + (x + 1)^r B(x)] \pmod{4}.$$

Mit Rücksicht auf

$$(x + 1)^{2^{n+1}} \equiv x^{2^{n+1}} + 2x^{2^n} + 1 \pmod{4}$$

erhält man

$$(6) \quad G(x) \equiv x^{2^{n+1}} + 2x^{2^n} + 1 + 2[(x + 1)^s A(x) + (x + 1)^r B(x)] \pmod{4}.$$

Durch Vergleichung von (5) und (6) ergibt sich

$$x^{2^{n+1}} + 1 \equiv x^{2^{n+1}} + 2x^{2^n} + 1 + 2[(x + 1)^s A(x) + (x + 1)^r B(x)] \pmod{4},$$

d. h.

$$x^{2^n} \equiv (x + 1)^s A(x) + (x + 1)^r B(x) \pmod{2},$$

was wegen der Eindeutigkeit der Faktorisierung mod 2 unmöglich ist. Damit ist der Beweis beendet.

Ich spreche meinen Dank Herrn Prof. Dr. L. RÉDEI für die Vereinfachung der Beweisführung aus.

(Eingegangen am 6. juni, 1953.)