Die Zerlegungsgesetze für die Primideale eines beliebigen algebraischen Zahlkörpers im Körper der l-ten Einheitswurzeln.

Von

Tonio Rella in Wien.

Es bedeute l eine ungerade Primzahl, $\zeta = e^{\frac{2\pi i}{l}}$, k sei ein algebraischer Zahlkörper, der mit dem Körper der l-ten Einheitswurzeln einen Körper vom Grade m (Teiler von $l-1$) gemein hat. Dann ist der aus k und ζ zusammengesetzte Körper (k, ζ) vom Relativgrad $\frac{l-1}{m}$ über k. Die Zerlegung der Primideale von k in (k, ζ) wird durch folgende zwei Gesetze bestimmt:

1. Ist p eine von l verschiedene Primzahl, $\mathfrak{p}$ ein in p aufgehendes Primideal von k vom Grade f, gehört ferner p nach dem Modul l zum Exponenten f_0 und ist ff' das kleinste gemeinschaftliche Vielfache von f und f_0, so zerfällt $\mathfrak{p}$ in (k, ζ) in z' Primideale vom Relativgrad f', wenn $\frac{l-1}{m} = f'z'$.

2. Ist $\mathfrak{l}$ ein in l aufgehendes Primideal von k vom Grade f und der Ordnung e, d der größte gemeinschaftliche Teiler von e und $l-1$, n die größte ganze Zahl, für welche eine Kongruenz gilt

$$-l \equiv \alpha^n (\mathfrak{l}^{e+1}),$$

wobei α eine ganze Zahl von k bedeutet, d_1 der größte gemeinschaftliche Teiler von n und $l-1$, so ist m ein Teiler von d_1 und d_1 ein Teiler von d und wenn

$$d = f' d_1 = f' z' m$$

gesetzt wird, so wird $\mathfrak{l}$ in (k, ζ) zerlegt in

$$\mathfrak{l} = (\mathfrak{L}\mathfrak{L}_1, \ldots, \mathfrak{L}_{z'-1})^{\frac{l-1}{d}}, \qquad N_k \mathfrak{L}_i = \mathfrak{l}^{f'},$$

wobei N_k die bezüglich k genommene Norm bedeutet.

Beweis für 1.

Jede für den Bereich von p ganze Zahl[1]) von (k, ζ) hat die Gestalt

$$(1) \qquad \mathsf{A} = \alpha_0 + \alpha_1 \zeta + \dots + \alpha_{n-1} \zeta^{n-1}, \qquad n = \frac{l-1}{m},$$

wobei die α_i für den Bereich von p ganze Zahlen von k bedeuten; denn in der Gestalt (1) ist jede Zahl von (k, ζ) darstellbar, wenn die α_i Zahlen von k sind. Ist aber A für den Bereich von p ganz, so sind auch die zu A relativ konjugierten Zahlen für den Bereich von p ganz und die α_i stellen sich als Brüche dar, deren Zähler für den Bereich von p ganz und deren Nenner ganz ist und in einer Potenz von l aufgeht, daher zu p teilerfremd ist.

Es sei $\mathfrak{p}$ ein in p aufgehendes Primideal von k,

$$N\mathfrak{p} = p^f = P$$

f' die kleinste positive Zahl, für welche

$$(2) \qquad P^{f'} \equiv 1 \pmod{l}$$

gilt.

Andererseits ist nach Voraussetzung f_0 die kleinste positive Zahl, für welche

$$(3) \qquad p^{f_0} \equiv 1 \pmod{l}$$

gilt, dann ist ersichtlich ff' das kleinste gemeinschaftliche Vielfache von f und f_0.

Aus (1) folgt, daß für jede für den Bereich von p ganze Zahl A

$$(4) \qquad \mathsf{A}^{p^{ff'}} \equiv \mathsf{A} \, (\mathfrak{P})$$

folgt, wenn $\mathfrak{P}$ ein in $\mathfrak{p}$ aufgehendes Primideal von (k, ζ) bedeutet. $\mathfrak{p}$ kann in (k, ζ) nur in verschiedene Primideale zerfallen, da $\mathfrak{p}$ in der Relativdiskriminante von (k, ζ) bezüglich k nicht aufgehen kann; es sei F der Grad von $\mathfrak{P}$, dann folgt aus (4), da diese Kongruenz für jede ganze Zahl von (k, ζ) gilt,

$$p^{ff'} \geqq p^F, \quad \text{also} \quad ff' \geqq F.$$

Andererseits folgt für $\mathsf{A} = \zeta$ aus dem Fermatschen Satz

$$\zeta^{p^F - 1} \equiv 1 \, (\mathfrak{P})$$

und daher

$$p^F \equiv 1 \pmod{l},$$

also F ein Vielfaches von f_0.

[1]) Für den Bereich von p heißt eine Zahl ganz, wenn sie als Bruch mit zu p teilerfremdem Nenner dargestellt werden kann.

Weil aber schließlich (k, ζ) ein (relativ zyklischer) Körper über k ist, muß F auch ein Vielfaches von f sein, und daraus folgt die Behauptung, weil ff' das kleinste gemeinschaftliche Vielfache von f und f_0 ist und $F \leqq ff'$.

Beweis für 2.

Es gelte in k die Zerlegung.

(5) $$l = \mathfrak{l}^e \mathfrak{a}, \quad (\mathfrak{a}, \mathfrak{l}) = 1, \qquad N\mathfrak{l} = l^f;$$

im Körper der l-ten Einheitswurzeln gilt

(6) $$l = \mathfrak{l}_0^{\,l-1}, \qquad N\mathfrak{l}_0 = l, \qquad \mathfrak{l}_0 = (1-\zeta).$$

Da k mit dem Körper ζ einen Unterkörper vom Grade m gemein haben soll, so muß e ein Vielfaches von m sein. Es sei

(7) $$d = (l-1, e) = m m'.$$

In (k, ζ) werde nun $\mathfrak{l}$ weiter zerlegt in

(8) $$\mathfrak{l} = (\mathfrak{L}\mathfrak{L}_1 \ldots \mathfrak{L}_{z'-1})^{g'}, \qquad N_k \mathfrak{L}_i = \mathfrak{l}^{f'},$$

daher

(9) $$l = \mathfrak{L}^{g'e}\mathfrak{A}, \qquad \mathfrak{A} \text{ ein zu } \mathfrak{L} \text{ teilerfremdes Ideal.}$$

Da aber (k, ζ) ein Oberkörper von ζ ist, so muß $g'e$ ein Vielfaches von $l-1$ und daher g' ein Vielfaches von $\frac{l-1}{d}$ sein. Es sei

(10) $$g' = \frac{l-1}{d}\, e',$$

also

$$\frac{l-1}{d} \cdot e' \cdot f' \cdot z' = \frac{l-1}{m} = \frac{l-1}{d}\, m',$$

folglich

(11) $$m' = e'f'z'.$$

Bedeutet r eine primitive Kongruenzwurzel von l, s die Permutation $\zeta \mid \zeta^r$, $s_1 = s^m$, so ist die Gruppe von (k, ζ) bezüglich k gleich $s_1^{x_1}$, $x_1 = 0, 1, \ldots, \frac{l-1}{m} - 1$, die Zerlegungsgruppe von $\mathfrak{L}$ bezüglich k gleich $s_1^{z'x_2}$, $x_2 = 0, 1, \ldots, \frac{l-1}{mz'} - 1$, die Trägheitsgruppe von $\mathfrak{L}$, bezüglich k gleich $s_1^{z'f'x_3}$, $x_3 = 0, 1, \ldots, \frac{l-1}{mf'z'} - 1$.

Aus (5) und (8) folgt

(12) $$N\mathfrak{L} = l^{ff'}.$$

Nun bedeute H eine primitive Kongruenzwurzel von $\mathfrak{L}$ so daß also $l^{ff'} - 1$ die niedrigste positive Potenz von H ist, für die

(13) $$\mathsf{H}^{l^{ff'}} \equiv 1(\mathfrak{L})$$

gilt.

Es sei η eine primitive Kongruenzwurzel von $\mathfrak{l}$ in k, für welche daher $l^f - 1$ der niedrigste positive Exponent ist, so daß

$$(14)\qquad \eta^{l^f-1} \equiv 1\,(\mathfrak{l}),$$

und ich kann und will annehmen, daß

$$(15)\qquad \eta \equiv \mathsf{H}^{\frac{l^{ff'}-1}{l^f-1}}\,(\mathfrak{L}).$$

Aus $\lambda_0 = 1-\zeta$ folgt

$$0 = \frac{1-\zeta^l}{1-\zeta} = \frac{1-(1-\lambda_0)^l}{\lambda_0} = l - \binom{l}{2}\lambda_0 + \dots + \lambda_0^{l-1}$$

und daher

$$(16)\qquad l \equiv -\lambda_0^{l-1}\,(\mathfrak{l}_0^l).$$

In k soll die Kongruenz gelten

$$(17)\qquad -l \equiv \eta^x \lambda^e\,(\mathfrak{l}^{e+1}),\quad (\lambda \text{ eine durch } \mathfrak{l} \text{ aber nicht durch } \mathfrak{l}^2 \text{ teilbare ganze Zahl von } k)$$

und in (k, ζ) sei

$$(18)\qquad \lambda \equiv \mathsf{H}^y \varLambda^{\frac{l-1}{d}e'}\,\left(\mathfrak{L}^{\frac{l-1}{d}e'+1}\right)$$

und

$$(19)\qquad \lambda_0 \equiv \mathsf{H}^u \varLambda^{\frac{ee'}{d}}\,\left(\mathfrak{L}^{\frac{ee'}{d}+1}\right),$$

wobei $\varLambda$ eine durch $\mathfrak{L}$ aber nicht durch $\mathfrak{L}^2$ teilbare ganze Zahl von (k, ζ) bedeutet.

Die Permutation s kann so gewählt werden, daß für die Permutation $s_2 = s_1^{z'}$, welche durch ihre Potenzen die Zerlegungsgruppe von $\mathfrak{L}$ bezüglich k erzeugt,

$$(20)\qquad s_2 \mathsf{H} \equiv \mathsf{H}^{l^f}\,(\mathfrak{L})$$

gilt.

Für die primitive Kongruenzwurzel r gilt eine Kongruenz

$$(21)\qquad r \equiv \mathsf{H}^{t\frac{l^{ff'}-1}{l-1}}\,(\mathfrak{L}),$$

wobei $(t, l-1) = 1$.

Es ist nun $s_3 = s_1^{z''f'}$ eine Permutation der Trägheitsgruppe von $\mathfrak{L}$ bezüglich k, daher gilt eine Kongruenz

$$(22)\qquad s_3 \varLambda \equiv \mathsf{H}^{\varrho} \varLambda\,(\mathfrak{L}^2),$$

und aus $s_3^{\frac{l-1}{d}e'} = 1$ folgt

$$\varLambda \equiv \mathsf{H}^{\varrho\frac{l-1}{d}e'} \varLambda\,(\mathfrak{L}^2),$$

daher

$$\varrho\,\frac{l-1}{d}\,e' \equiv 0 \pmod{l^{ff'}-1}. \tag{23}$$

Andrerseits folgt aus (19) und (21)

$$s_3\lambda_0 = r^{mz'f'}\lambda_0 = \mathsf{H}^{tmz'f'\frac{l^{ff'}-1}{l-1}}\lambda_0 = \mathsf{H}^{\frac{ee'}{d}\varrho}\lambda_0(\mathfrak{L}^{\frac{ee'}{d}+1}),$$

$$\varrho\,\frac{ee'}{d} \equiv tmz'f'\,\frac{l^{ff'}-1}{l-1} \pmod{l^{ff'}-1}. \tag{24}$$

Wird (23) mit e und (24) mit $l-1$ multipliziert und beide Kongruenzen nach dem Modul $d(l^{ff'}-1)$ genommen, so folgt

$$tmz'f'(l^{ff'}-1) \equiv 0 \pmod{d(l^{ff'}-1)},$$

$$tmz'f' \equiv 0 \pmod{d = me'f'z'},$$

$$t \equiv 0 \pmod{e'}; \tag{25}$$

e' ist ein Teiler von $l-1$, t zu $l-1$ teilerfremd, daher

$$e' = 1. \tag{26}$$

Es sei ferner

$$s_2\Lambda = \mathsf{H}^{\sigma}\Lambda(\mathfrak{L}^2), \tag{27}$$

dann folgt aus (18) und (20) wegen $s_2\lambda = \lambda$

$$\lambda \equiv \mathsf{H}^{yl^f+\sigma\frac{l-1}{d}}\Lambda^{\frac{l-1}{d}} = \mathsf{H}^{y(l^f-1)+\sigma\frac{l-1}{d}}\lambda(\mathfrak{L}^{\frac{l-1}{d}+1}), \tag{28}$$

daher

$$y(l^f-1)+\sigma\,\frac{l-1}{d} \equiv 0 \pmod{l^{ff'}-1}. \tag{29}$$

Aus (19) folgt wegen $s_2\lambda_0 = r^{mz'}\lambda_0(\mathfrak{l}_0^2)$

$$s_2\lambda_0 \equiv \mathsf{H}^{tmz'\frac{l^{ff'}-1}{l-1}}\lambda_0 = \mathsf{H}^{u(l^f-1)+\sigma\frac{e}{d}}\lambda_0(\mathfrak{L}^{\frac{e}{d}+1}),$$

daher

$$u(l^f-1)+\sigma\,\frac{e}{d} \equiv tmz'\,\frac{l^{ff'}-1}{l-1} \pmod{l^{ff'}-1}; \tag{30}$$

und aus (16), (17), (18) und (19) folgt schließlich

$$-l \equiv \eta^x\lambda^e = \mathsf{H}^{x\frac{l^{ff'}-1}{l^f-1}+ey}\Lambda^{\frac{(l-1)e}{d}} = \mathsf{H}^{u(l-1)}\Lambda^{\frac{(l-1)e}{d}}(\mathfrak{L}^{\frac{(l-1)e}{d}+1}),$$

daher

$$x\,\frac{l^{ff'}-1}{l^f-1}+ey \equiv u(l-1) \pmod{l^{ff'}-1}. \tag{31}$$

Multipliziere ich (31) mit l^f-1, (30) mit $l-1$, (29) mit e, betrachte alle Kongruenzen nach dem Modul $d(l^{ff'}-1)$ und addiere alle drei Kongruenzen ((29) mit vertauschten Seiten), so folgt

$$x(l^{ff'}-1) \equiv tmz'(l^{ff'}-1) \pmod{d(l^{ff'}-1)}, \tag{32}$$

$$x \equiv tmz' \pmod{d}; \tag{33}$$

mz' ist ein Teiler von d, t ist zu $l-1$ und daher auch zu d teilerfremd. Setze ich

$$x = mz'x_1, \quad d = mz'f',$$

so folgt aus (33), daß x_1 und f' teilerfremd sein müssen und es gilt eine Kongruenz

$$-l \equiv \eta^x \lambda^e \equiv \left(\eta^{x_1} \lambda^{\frac{e}{d} f'}\right)^{mz'} (\mathfrak{l}^{e+1}). \tag{34}$$

Ist andererseits

$$-l \equiv \alpha^n (\mathfrak{l}^{e+1}), \tag{35}$$

so muß für α eine Kongruenz gelten

$$\alpha \equiv \eta^a \lambda^{\frac{e}{n}} \left(\mathfrak{l}^{\frac{e}{n}+1}\right), \quad \left(\frac{e}{n} \text{ eine ganze Zahl}\right) \tag{36}$$

$$-l \equiv \alpha^n \equiv \left(\eta^a \lambda^{\frac{e}{n}}\right)^n (\mathfrak{l}^{e+1}). \tag{37}$$

Da aber n die größte ganze Zahl sein soll, für welche eine Kongruenz der Gestalt (35) gilt, so muß n ein Vielfaches von mz' sein

$$n = mz'n_1$$

und durch Vergleich von (34) und (33) folgt weiter

$$an_1 \equiv x_1 \pmod{l^f - 1}.$$

Da x_1 zu f' teilerfremd ist und f' ein Teiler von $l^f - 1$, so muß daher auch n_1 zu f' teilerfremd sein und daher ist

$$d_1 = (n, l-1) = (n, e, l-1) = (n, d) = mz'(n_1, f') = mz', \tag{38}$$

womit die Behauptung erwiesen ist.

(Eingegangen am 24. Februar 1919.)