XLII.

Grundideale von Kreiskörpern.

Es sei m eine natürliche Zahl, die im folgenden stets beibehalten wird. Ist a ein Divisor von m, so soll mit

$$\varepsilon a$$

der Inbegriff aller ganzen rationalen Zahlen bezeichnet werden, welche relative Primzahlen zu m (also auch zu a) und $\equiv 1 \pmod{a}$ sind. Dieser Inbegriff besteht aus

$$\frac{\varphi(m)}{\varphi(a)}$$

Klassen (mod. m), und diese Klassen bilden eine Gruppe, welche selbst mit εa bezeichnet werden soll.

Hiernach ist $\varepsilon 1$ der Inbegriff aller relativen Primzahlen zu m, welcher aus $\varphi(m)$ Klassen besteht. Ebenso ist εm die Hauptklasse.

$$(\varepsilon m, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)}; \quad (\varepsilon a, \varepsilon 1) = \varphi(a).$$

Sind a, b Divisoren von m, c ihr kleinstes gemeinsames Vielfaches, d ihr größter gemeinsamer Teiler, also $ab = cd$, so ist

εd das kleinste gemeinsame Vielfache
εc der größte gemeinsame Teiler } der Gruppen $\varepsilon a, \varepsilon b$,

$$\varepsilon d = \varepsilon a \cdot \varepsilon b,$$
$$\varepsilon c = \varepsilon a \mid \varepsilon b,$$

wo $\mid$ das Zeichen für den größten gemeinsamen Teiler von Gruppen ist. Ist H irgendeine in $\varepsilon 1$ als Teiler enthaltene Gruppe, so ist das kleinste gemeinsame Vielfache aller in H enthaltenen Gruppen von der Form εa selbst eine solche Gruppe εd, wo d der größte gemeinsame Teiler aller a. Diese Zahl d heißt der Exponent der Gruppe H. Also: Ist a teilbar durch d, so ist εa in H enthalten; ist a nicht teilbar durch d, so ist εa nicht in H enthalten.

Es sei θ eine primitive Wurzel der Gleichung $\theta^m = 1$; $K(m) = R(\theta)$ sei der durch θ erzeugte vollständige Kreiskörper vom Grade $\varphi(m)$; dieser gehört zur Gruppe $\varepsilon m \equiv 1 \pmod{m}$.

Es sei $\mathfrak{Q}$ ein Divisor von $K(m)$, zur Gruppe H gehörig und vom Grade $n = (H, \varepsilon 1)$. Durchläuft h alle in H enthaltenen $\frac{\varphi(m)}{n}$ Klassen, so ist

$$f(x) = \Pi(x - \theta^h)$$

die in $\mathfrak{Q}$ irreduzibele Funktion von x, welche für $x = \theta$ verschwindet, und das Grundideal von $K(m)$ in bezug auf $\mathfrak{Q}$ ist ($\sim$ bedeutet: assoziiert mit)

$$\sim f'(\theta) = \Pi(\theta - \theta^h) \sim \Pi(1 - \theta^{h-1}), \quad \text{mit Ausschluß von } h \equiv 1 \pmod{m}.$$

Jeder Faktor $(1 - \theta^{h-1})$ ist nur dann keine Einheit, sondern Faktor einer in m aufgehenden natürlichen Primzahl p, wenn der kleinste Nenner des Bruches $\frac{h-1}{m}$ eine Potenz von p ist; und zwar ist gleichzeitig (Modul-Bezeichnung)

$$\left[1, \frac{h-1}{m}\right] = \left[\frac{1}{p^s}\right] \text{ mit } 1 - \theta^{h-1} \sim p^{\frac{1}{\varphi(p^s)}}; \quad s > 0.$$

Nun sei m' der größte durch p nicht teilbare Divisor von

$$m = m' p^k; \quad k > 0.$$

Damit eine Zahl h der vorstehenden Bedingung genüge, ist erforderlich

$$h \equiv 1 \left(\text{mod.} \frac{m}{p^s} = m' p^{k-s}\right), \quad h - 1 = u \cdot m' p^{k-s},$$

wo, wenn $s > 0$ ist, u nicht teilbar durch p; d. h. h muß eine Zahl der Gruppe $\varepsilon \frac{m}{p^s}$ sein, also ein Element des größten gemeinsamen Teilers

$$Q_s = H \mid \varepsilon \frac{m}{p^s}$$

der Gruppen H und $\varepsilon \frac{m}{p^s}$; es sei

$$q_s = (\varepsilon m, Q_s)$$

der Grad von Q_s. Es darf aber h nicht $\equiv 1 \left(\text{mod.} \frac{m}{p^{s-1}} = \frac{m}{p^s} \cdot p\right)$, also nicht in $\varepsilon \frac{m}{p^{s-1}}$ enthalten, also keine der q_{s-1} Zahlen in Q_{s-1} sein. Mithin ist $q_s - q_{s-1}$ die Anzahl der obigen h, und folglich ist der betreffende Faktor von $f'(\theta)$, welcher nur Faktoren von p enthält,

$$\sim p^{\frac{q_1 - q_0}{\varphi(p)} + \frac{q_2 - q_1}{\varphi(p^2)} + \frac{q_3 - q_2}{\varphi(p^3)} + \cdots + \frac{q_k - q_{k-1}}{\varphi(p^k)}}.$$

Offenbar ist

$$Q_0 = \varepsilon m, \quad q_0 = 1.$$

Der Grad der Gruppe $\varepsilon \frac{m}{p^s}$ ist

$$\frac{\varphi(m)}{\varphi\left(\frac{m}{p^s}\right)} = \frac{\varphi(m')\varphi(p^k)}{\varphi(m')\varphi(p^{k-s})} = \frac{\varphi(p^k)}{\varphi(p^{k-s})} = p^s \text{ oder } = \varphi(p^k) = p^k - p^{k-1},$$

je nachdem $s < k$ oder $s = k$.

Also ist q_s Divisor von p^s, wenn $s < k$, und q_k Divisor von $\varphi(p^k)$. Außerdem ist Q_s Divisor von Q_{s+1}, also auch q_s Divisor von q_{s+1}. Ferner ist

$$\left(Q_s, \ \varepsilon \frac{m}{p^s}\right) = \left(H, \ \varepsilon \frac{m}{p^s}\right) = \left(H, H\varepsilon \frac{m}{p^s}\right),$$

$$q_s \left(H, H\varepsilon \frac{m}{p^s}\right) = (\varepsilon m, Q_s)\left(Q_s, \ \varepsilon \frac{m}{p^s}\right) = \left(\varepsilon m, \ \varepsilon \frac{m}{p^s}\right) = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$\frac{q_1}{p} = \frac{1}{\left(H, \varepsilon \frac{m}{p}\right)}, \quad \frac{q_2}{p^2} = \frac{1}{\left(H, \varepsilon \frac{m}{p^2}\right)}, \ \cdots, \quad \frac{q_{k-1}}{p^{k-1}} = \frac{1}{\left(H, \varepsilon \frac{m}{p^{k-1}}\right)},$$

$$\frac{q_k}{\varphi(p^k)} = \frac{1}{\left(H, \varepsilon \frac{m}{p^k}\right)}, \quad \frac{q_0}{1} = \frac{1}{(H, \varepsilon m)} = 1.$$

Ist Ω der Körper $R = K(1)$ der rationalen Zahlen, so ist $H = \varepsilon 1$ die Gesamtgruppe, mithin $Q_s = \varepsilon \frac{m}{p^s}$, und

$$q_s = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$q_k - q_{k-1} = \varphi(p^k) - p^{k-1} = (p-2)p^{k-1} = \frac{p-2}{p-1}\varphi(p^k),$$

$$q_{k-1} - q_{k-2} = p^{k-1} - p^{k-2} = \varphi(p^{k-1}), \quad q_{k-2} - q_{k-3} = \varphi(p^{k-2});$$

$$\cdots q_1 - q_0 = p - 1 = \varphi(p),$$

und folglich wird

$$p^{k-1+\frac{p-2}{p-1}} = p^{k-\frac{1}{p-1}}$$

der betreffende Faktor des absoluten (d. h. nach R genommenen) Grundideals von $K(m)$.

Wenn Ω und H wieder die allgemeine Bedeutung haben, so ist daher

$$p^{k-\frac{1}{p-1}-\frac{q_1-q_0}{\varphi(p)}-\frac{q_2-q_1}{\varphi(p^2)}-\cdots-\frac{q_k-q_{k-1}}{\varphi(p^k)}}$$

$$= p^{k-\frac{q_1}{p}-\frac{q_2}{p^2}-\cdots-\frac{q_{k-1}}{p^{k-1}}-\frac{q_k}{\varphi(p^k)}}$$

$$= p^{\Sigma\left(1-\frac{1}{\left(H,\ \varepsilon\frac{m}{p^s}\right)}\right)} = p^{\Sigma\left(1-\frac{1}{\left(\Omega,\ K\left(\frac{m}{p^s}\right)\right)}\right)}$$

der betreffende Faktor des Grundideals des Körpers Ω nach R.

Da alle $\varepsilon\frac{m}{p^s}$ Teiler der Gruppe $\varepsilon\frac{m}{p^k} = \varepsilon m'$ sind, so ist Q_s auch der gr. g. T. von H, $\varepsilon\frac{m}{p^s}$ und $\varepsilon m'$, also auch Q_s der gr. g. T. von Q_k und $\varepsilon\frac{m}{p^s}$.

Ist ψ ein Charakter der Abelschen Gruppe $\varepsilon 1$, so soll ψ_0 die Gruppe aller derjenigen Elemente r von $\varepsilon 1$ bedeuten, für welche $\psi(r) = 1$ ist, und unter dem Exponenten von ψ soll der Exponent der Gruppe ψ_0 verstanden sein.

Ist H irgendein Teiler von $\varepsilon 1$ und (wie oben) Ω der zugehörige Körper vom Grade $n = (H, \varepsilon 1)$, so ist n die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind.

Es soll das Produkt der Exponenten dieser n Charaktere ψ oder vielmehr die höchste in demselben aufgehende Potenz von p ermittelt werden.

Es sei ψ einer dieser n Charaktere und sein Exponent $= m'' p^{k-s}$, wo m'' nicht teilbar durch p, also Divisor von m', und $0 \leqq s < k$.

Dann ist $\varepsilon m'' p^{k-s}$ Teiler von ψ_0, also auch $\varepsilon m' p^{k-s} = \varepsilon\frac{m}{p^s}$ Teiler von ψ_0; also ist auch $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0.

Umgekehrt aber, wenn $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0, so ist der Exponent von ψ_0 ein Divisor von $\frac{m}{p^s}$, und die höchste in ihm aufgehende Potenz von p ist Divisor von p^{k-s}.

Nun ist $\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)$ die Anzahl aller dieser ψ, also ebenso $\left(H\,\varepsilon\,\frac{m}{p^{s+1}},\,\varepsilon\,1\right)$ die Anzahl aller ψ, deren Exponent höchstens durch p^{k-s-1} teilbar ist, also $\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)-\left(H\,\varepsilon\,\frac{m}{p^{s+1}},\,\varepsilon\,1\right)$ die Anzahl derjenigen ψ, deren Exponent die Potenz p^{k-s} genau enthält.

Nun ist

$$(H,\,\varepsilon\,1)=\left(H,\,H\,\varepsilon\,\frac{m}{p^s}\right)\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)=n;$$

und

$$q_s\left(H,\,H\,\varepsilon\,\frac{m}{p^s}\right)=\frac{\varphi\,(p^k)}{\varphi\,(p^{k-s})},$$

folglich

$$\frac{\varphi\,(p^k)}{\varphi\,(p^{k-s})}\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)=n\,q_s,\quad \left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)=n\,q_s\,\frac{\varphi\,(p^{k-s})}{\varphi\,(p^k)}$$

$$=\frac{n\,q_s}{p^s}\text{ oder }=\frac{n\,q_k}{\varphi\,(p^k)},$$

je nachdem

$$s<k\quad\text{oder}\quad s=k.$$

Also ist

1	$\frac{n\,q_{k-1}}{p^{k-1}}-\frac{n\,q_k}{\varphi\,(p^k)}$	Anzahl der ψ, in deren Exponent der Faktor p,
2	$\frac{n\,q_{k-2}}{p^{k-2}}-\frac{n\,q_{k-1}}{p^{k-1}}$	„ „ „ „ „ „ „ „ p^2;
$k-1$	$\frac{n\,q_1}{p}-\frac{n\,q_2}{p^2}$	„ „ „ „ „ „ „ „ p^{k-1};
k	$n-\frac{n\,q_1}{p}$	„ „ „ „ „ „ „ „ p^k.

Also

$$p^{kn-\frac{nq_1}{p}-\frac{nq_2}{p^2}-\cdots-\frac{nq_{k-1}}{p^{k-1}}-\frac{nq_k}{\varphi(p^k)}}=\left(p^{k-\frac{q_1}{p}-\frac{q_2}{p^2}-\cdots-\frac{q_{k-1}}{p^{k-1}}-\frac{q_k}{\varphi(p^k)}}\right)^n.$$

Mithin ist dies Produkt aller Exponenten der n Charaktere ψ des Körpers Ω zugleich die n^{te} Potenz des Grundideals von Ω, d. h. $=\pm$ Grundzahl von Ω, w. z. b. w. (Norm des Grundideals.)

Erläuterungen. 1. Ist die Gruppe H von Elementen h irgendein Teiler der Gruppe $\varepsilon\,1$, so ist

$$(H,\,\varepsilon\,1)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche Multipla des identischen (oder Haupt-) Charakters der Gruppe H sind, welche also für alle Elemente h der Gruppe H der Bedingung

$$\psi(h) = 1$$

genügen; oder mit anderen Worten: $(H, \varepsilon 1)$ ist die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind, also der Bedingung

$$(\psi_0, H) = 1$$

genügen.

2. Ist a (wie auf S. 401) irgendein Divisor von m, und εa wieder die Gruppe von $\frac{\varphi(m)}{\varphi(a)}$ Klassen (mod. m), deren Zahlen relative Primzahlen zu m und zugleich $\equiv 1 \pmod{a}$ sind, so ist die Aussage

$$(H, \varepsilon a) = 1 \quad \text{(also } \varepsilon a \text{ Teiler von } H)$$

gleichbedeutend damit, daß der Exponent d der Gruppe H ein Divisor von a ist.

3. Speziell bedeutet also die Aussage

$$(\psi_0, \varepsilon a) = 1,$$

daß der Exponent des Charakters ψ (d. h. der Exponent der Gruppe ψ_0) Divisor von a ist.

4. Das System der beiden gleichzeitigen Aussagen

$$(\psi_0, H) = 1, \quad (\psi_0, \varepsilon a) = 1$$

ist gleichbedeutend mit der einen Aussage

$$(\psi_0, H \varepsilon a) = 1;$$

diese letztere bedeutet also, daß erstens ψ ein Multiplum des Hauptcharakters der Gruppe H [also $\psi(h) = 1$ für alle h], und daß zweitens der Exponent von ψ ein Divisor von a ist; zufolge 1. (wenn dort H durch $H \varepsilon a$ ersetzt wird) ist

$$(H \varepsilon a, \varepsilon 1) \quad \text{die Anzahl} = f(a)$$

aller dieser Charaktere.

5. Bedeutet daher, wenn a irgendein Divisor von m, und H eine feste Gruppe ist,

$$f'(a)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche

Multipla des Hauptcharakters von H sind, und deren Exponent $= a$ ist, so ist die über alle Divisoren d von a erstreckte Summe

$$\sum f'(d) = (H \varepsilon a, \varepsilon 1) = f(a)$$

und folglich umgekehrt

$$f'(a) = \sum \eta\left(\frac{a}{d}\right)(H \varepsilon d, \varepsilon 1) = \sum \eta\left(\frac{a}{d}\right) f(d),$$ d alle Divisoren von a,

wo η die Funktion von Mertens-Cantor bedeutet.

6. Das Produkt der Exponenten aller Charaktere ψ, welche Multipla des Hauptcharakters der Gruppe sind, und deren Anzahl zufolge 1. $= (H, \varepsilon 1)$ ist, ist daher das über alle Divisoren a von m ausgedehnte Produkt

$$\Pi a^{f'(a)}.$$

7. Setzt man

$$n = (H, \varepsilon 1),$$

so ist

$$n = (H, H \varepsilon a)(H \varepsilon a, \varepsilon 1); \quad (H \varepsilon a, \varepsilon 1) = \frac{n}{(H, H \varepsilon a)};$$

ferner ist

$$(H, H \varepsilon a) = (H, \varepsilon a) = (H \mid \varepsilon a, \varepsilon a),$$

wo $A \mid B$ allgemein den größten gemeinsamen Teiler der Gruppen A, B bedeutet; immer ist $(A, B) = (A, AB) = (A \mid B, B)$. Ferner ist

$$(\varepsilon m, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)} = (\varepsilon m, H \mid \varepsilon a)(H \mid \varepsilon a, \varepsilon a);$$

bezeichnet man daher

$$(\varepsilon m, H \mid \varepsilon a) = t(a),$$

welches der Grad des größten gemeinsamen Teilers $H \mid \varepsilon a$ der beiden Gruppen H und εa ist, so wird

$$(H \mid \varepsilon a, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)} \cdot \frac{1}{t(a)}; \quad (H \varepsilon a, \varepsilon 1) = \frac{n}{\varphi(m)} \cdot \varphi(a) t(a) = f(a).$$

Außerdem ist

$$\varphi(m) = (\varepsilon m, \varepsilon 1) = (\varepsilon m, H)(H, \varepsilon 1) = (\varepsilon m, H) n; \quad \frac{\varphi(m)}{n} = (\varepsilon m, H).$$

8. Es werden nur noch solche Charaktere ψ der Gruppe $\varepsilon 1$ betrachtet, welche Multipla des Hauptcharakters der Gruppe H sind, also der Bedingung $(\psi_0, H) = 1$ genügen und deren Anzahl $= n = (H, \varepsilon 1)$ ist.

Ist nun p eine in m aufgehende natürliche Primzahl und

$$m = m' p^k, \quad k > 0, \quad m' \text{ nicht teilbar durch } p,$$

so ist

$$\left(H \varepsilon \frac{m}{p^s}, \varepsilon 1\right), \quad \text{wo } 0 \leqq s \leqq k,$$

die Anzahl derjenigen Charaktere ψ, deren Exponenten Divisoren von

$$\frac{m}{p^s} = m' p^{k-s}$$

sind. Also

$(H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von m'	$= f(m')$
$(H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p$	$= f(m' p)$
$(H \varepsilon m' p^2, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^2$	$= f(m' p^2)$
. . . . .	. . . . .
$(H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^{k-1}$	$= f(m' p^{k-1})$
$n = (H \varepsilon m' p^k, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^k = m$	$= f(m' p^k) = f(m)$

$= (H \varepsilon m, \varepsilon 1)$

$= (H, \varepsilon 1)$.

Also ist

$(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p, nicht den Faktor p^2 enthalten,

$(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^2, nicht den Faktor p^3 enthalten,

. . . . . .

$(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^k, nicht den Faktor p^{k+1} enthalten.

Mithin ist der Exponent der höchsten im Produkte der Exponenten aller n Charaktere ψ aufgehenden Potenz von p

$$= \{(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)\} + 2\{(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)\} + \cdots + k\{(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= k(H, \varepsilon 1) - \{(H \varepsilon m', \varepsilon 1) + (H \varepsilon m' p, \varepsilon 1) + \cdots + (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= kn - \sum_{s=0}^{s=k-1} f(m' p^s).$$

Es ist aber

$$(H, \varepsilon\, 1) = (H, H\,\varepsilon\, m'\, p^s)(H\,\varepsilon\, m'\, p^s, \varepsilon\, 1) = (H, \varepsilon\, m'\, p^s)\, f(m'\, p^s),$$

also wird der Potenzexponent von p

$$= n\left\{k - \sum_{s=0}^{s=k-1} \frac{1}{(H, \varepsilon\, m'\, p^s)}\right\}.$$

Es ist aber

$$(H, \varepsilon\, m'\, p^s) = (H \,|\, \varepsilon\, m'\, p^s, \varepsilon\, m'\, p^s),$$

also

$$(\varepsilon\, m, H \,|\, \varepsilon\, m'\, p^s)(H, \varepsilon\, m'\, p^s) = (\varepsilon\, m, \varepsilon\, m'\, p^s) = \frac{\varphi(m)}{\varphi(m'\, p^s)} = \frac{\varphi(p^k)}{\varphi(p^s)},$$

also

$$\frac{1}{(H, \varepsilon\, m'\, p^s)} = \frac{(\varepsilon\, m, H \,|\, \varepsilon\, m'\, p^s)}{p^{k-s}}, \quad \text{wenn } s > 0,$$

und

$$\frac{1}{(H, \varepsilon\, m')} = \frac{(\varepsilon\, m, H \,|\, \varepsilon\, m')}{\varphi(p^k)}.$$

Also wird der obige Potenzexponent von p

$$= n\left\{k - \frac{(\varepsilon\, m, H \,|\, \varepsilon\, m')}{\varphi(p^k)} - \sum_{s=1}^{s=k-1} \frac{(\varepsilon\, m, H \,|\, \varepsilon\, m'\, p^s)}{p^{k-s}}\right\}.$$

Erläuterungen zur vorstehenden Abhandlung.

Es handelt sich um eine Anwendung der in XLI entwickelten allgemeinen Begriffe.

Der hier für den Kreiskörper gegebene Führer-Diskriminantensatz — Darstellung der Diskriminante als Produkt der Führer (Exponenten bei Dedekind) der Charaktere der zugehörigen Klassengruppe — ist im allgemeinen Fall der relativ-Abelschen Körper auf zwei verschiedene Arten erbracht: mit transzendenten Methoden (Heckesche L-Reihen mit Größencharakteren) und arithmetisch unter Benutzung des Umkehrsatzes der Klassenkörpertheorie (vgl. den Bericht von Hasse, I, II; Jahresber. d. d. Math.-Ver. **35** und Ergänzungsbd. VI).

Das Analogon für Galoissche, nicht Abelsche Körper hat neuerdings E. Artin aufgestellt (Journ. f. Math. **164** (1931)).

Noether.
