## § 8. Charaktere und ganz-algebraische Zahlen

**8.1. Definition.** Eine Zahl $x \in \mathbb{C}$ heißt *algebraisch*, wenn es rationale Zahlen $a_1, a_2, \ldots, a_n \in \mathbb{Q}$ gibt, so dass

$$(1) \qquad x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0.$$

Die Zahl $x$ heißt *ganz-algebraisch*, wenn man in der Gleichung (1) sogar $a_i \in \mathbb{Z}$ wählen kann.

In der algebraischen Zahlentheorie beweist man: Die Menge aller algebraischen Zahlen bildet einen Körper, die Menge aller ganz-algebraischen Zahlen bildet einen Ring, d.h. Summe und Produkt ganz-algebraischer Zahlen sind wieder ganz-algebraisch.

*Beispiel.* Sei $n \geq 2$ eine ganze Zahl. Dann ist die $n$-te Einheitswurzel $\zeta_n = e^{2\pi i/n}$ ganz-algebraisch, ebenso alle Elemente des Rings $\mathbb{Z}[\zeta_n]$.

**8.2. Satz.** *Eine Zahl $x \in \mathbb{Q}$, die ganz-algebraisch ist, liegt bereits in $\mathbb{Z}$.*

*Beweis.* Wir können annehmen, dass $x \neq 0$. Die Zahl $x$ genügt einer Gleichung

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \quad \text{mit} \quad a_1, \ldots, a_n \in \mathbb{Z}.$$

Wir schreiben $x = u/v$ mit teilerfremden ganzen Zahlen $u, v \in \mathbb{Z}$, $v > 0$. Multiplizieren wir die Gleichung mit $v^n$, so ergibt sich

$$u^n = -v(a_1 u^{n-1} + a_2 u^{n-2} v + \ldots + a_n v^{n-1}).$$

Wäre $v \neq 1$, so gäbe es eine Primzahl $p$ mit $p \mid v$. Aus der obigen Gleichung folgt dann $p \mid u$, im Widerspruch zur Teilerfremdheit von $u$ und $v$. Also ist $v = 1$, d.h. $x$ eine ganze Zahl, q.e.d.

**8.3. Satz.** *Sei $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ eine Darstellung einer endlichen Gruppe $G$ und $\chi$ der Charakter von $\varrho$. Dann sind alle Werte $\chi(x)$, $x \in G$, ganz-algebraische Zahlen.*

*Beweis.* Da $G$ endlich ist, hat jedes Element $x \in G$ endliche Ordnung, d.h. es gibt eine positive ganze Zahl $m$ mit $x^m = 1$. Daraus folgt $\varrho(x)^m = E$ und für alle Eigenwerte $\lambda$ von $\varrho(x)$ gilt ebenfalls $\lambda^m = 1$, also ist $\lambda$ ganz-algebraisch. Da $\chi(x) = \mathrm{Tr}(\varrho(x))$ die Summe der Eigenwerte von $\varrho(x)$ (mit Vielfachheiten) ist, ist auch $\chi(x)$ ganz-algebraisch.

**8.4. Satz.** *Sei $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ eine irreduzible Darstellung einer endlichen Gruppe $G$ und $\chi : G \to \mathbb{C}$ der Charakter von $\varrho$. Sei $g \in G$ und $\Gamma \subset G$ die Konjugationsklasse von $g$. Die Matrix $S$ werde definiert durch*

$$S := \sum_{x \in \Gamma} \varrho(x) \in M(n \times n, \mathbb{C}).$$

*Dann gilt*

$$S = \lambda E \quad \textit{mit} \quad \lambda = \frac{|\Gamma|}{n}\,\chi(g).$$

*Diese Zahl $\lambda$ ist ganz-algebraisch.*

*Beweis.* Sei $t \in G$ beliebig. Dann gilt

$$\varrho(t)S\varrho(t)^{-1} = \sum_{x\in\Gamma} \varrho(t)\varrho(x)\varrho(t)^{-1} = \sum_{x\in\Gamma} \varrho(txt^{-1}) = \sum_{y\in\Gamma} \varrho(y) = S,$$

d.h.

$$\varrho(t)S = S\varrho(t) \quad \text{für alle } t \in G.$$

Aus dem Schurschen Lemma folgt nun $S = \lambda E$ für ein $\lambda \in \mathbb{C}$. Um $\lambda$ zu berechnen, bilden wir von beiden Seiten der Gleichung $S = \lambda E$ die Spur. Es ist

$$\mathrm{Tr}(S) = \sum_{x\in\Gamma} \mathrm{Tr}(\varrho(x)) = \sum_{x\in\Gamma} \chi(x) = |\Gamma|\,\chi(g)$$

und $\mathrm{Tr}(\lambda E) = n\lambda$. Daraus folgt $\lambda = |\Gamma|\chi(g)/n$.

Um zu beweisen, dass $\lambda$ ganz-algebraisch ist, zeigen wir, dass $\lambda$ Eigenwert einer ganzzahligen Matrix $A \in M(N \times N, \mathbb{Z})$, $N = |G|$, ist. Denn dann ist $\lambda$ Nullstelle des charakteristischen Polynoms $\det(xE - A)$, was ein Polynom mit ganzzahligen Koeffizienten und höchstem Koeffizienten 1 ist.

Der zur Darstellung $\varrho$ gehörige Darstellungs-Modul ist isomorph zu einem minimalen Links-Ideal $I$ des Gruppenrings $\mathbb{C}[G]$. Sei

$$z = \sum_{x\in\Gamma} x \in \mathbb{C}[G].$$

Für jedes Element $u \in I$ gilt dann $z \cdot u = \lambda u$, d.h. $\lambda$ ist ein Eigenwert der linearen Abbildung

$$\Phi : \mathbb{C}[G] \longrightarrow \mathbb{C}[G], \quad v \mapsto z \cdot v.$$

Wir betrachten jetzt die Matrix $A$ von $\Phi$ bzgl. der Basis $(e_t)_{t\in G}$ von $\mathbb{C}[G]$. Es gilt

$$\Phi(e_t) = z \cdot e_t = \sum_{x\in\Gamma} e_{xt}.$$

Daraus folgt, dass alle Koeffizienten von $A$ gleich 1 oder 0 sind. Daher ist $\lambda$ als Eigenwert von $A$ ganz-algebraisch.

**8.5. Satz.** *Der Grad jeder irreduziblen Darstellung $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ einer endlichen Gruppe ist ein Teiler der Gruppenordnung $|G|$.*

*Beweis.* Es seien $g_1, g_2, \ldots, g_h$ Repräsentanten der Konjugationsklassen $\Gamma_1, \Gamma_2, \ldots, \Gamma_h$ von $G$. Sei $\chi$ der Charakter von $\varrho$. Nach Satz 8.4 sind die Zahlen

$$\frac{1}{n}\,|\Gamma_i|\,\chi(g_i)$$

ganz-algebraisch. Da auch $\overline{\chi(g_i)}$ ganz-algebraisch ist, folgt, dass auch

$$\frac{1}{n}\sum_{i=1}^{h}|\Gamma_i|\chi(g_i)\overline{\chi(g_i)} = \frac{1}{n}\cdot|G|\cdot\|\chi\|^2 = \frac{|G|}{n}$$

ganz-algebraisch ist. Da $|G|/n$ aber offensichtlich rational ist, muss $|G|/n$ nach Satz 8.2 sogar ganz sein, d.h. $n$ ist ein Teiler von $|G|$, q.e.d.

Für den nächsten Satz erinnern wir an den Begriff der *einfachen Gruppe*. Eine Gruppe $G$ heißt einfach, wenn $G$ nur die trivialen Normalteiler $\{1\}$ und $G$ besitzt. Eine endliche abelsche Gruppe ist genau dann einfach, wenn sie Primzahl-Ordnung hat. Interessanter sind die nicht-abelschen einfachen Gruppen. Die kleinste solche Gruppe ist $A_5$, die Gruppe der geraden Permutationen einer Menge von fünf Elementen.

**8.6. Satz.** *Sei $G$ eine endliche einfache Gruppe. Dann besitzt $G$ keine nicht-triviale Darstellung $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ vom Grad $n < 3$.*

*Beweis.* Jede nicht-triviale Darstellung $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ ist treu, denn $\mathrm{Ker}(\varrho)$ ist ein Normalteiler von $G$. Gäbe es eine nicht-triviale Darstellung vom Grad 1, müsste deshalb $G$ abelsch sein, Widerspruch!

Nehmen wir nun an, $G$ besitzt eine nicht-triviale Darstellung $\varrho$ vom Grad 2. Dann ist $\varrho$ irreduzibel, denn andernfalls zerfiele $\varrho$ in zwei Darstellungen vom Grad 1. Wir dürfen annehmen, dass $\varrho : G \to U(2)$ unitär ist. Die Abbildung $\det(\varrho) : G \to \mathbb{C}^*$ ist eine Darstellung vom Grad 1, also trivial, d.h. $\det(\varrho(x)) = 1$ für alle $x \in G$. Also ist $\varrho$ sogar eine injektive Abbildung $\varrho : G \to SU(2)$ in die spezielle unitäre Gruppe. Nach Satz 8.5 ist die Ordnung von $G$ gerade, also besitzt $G$ ein Element $s$ der Ordnung 2 (Satz von Cauchy, Spezialfall der Sylowschen Sätze). Da $\varrho$ injektiv ist, muss die Matrix $S := \varrho(s) \in SU(2)$ ebenfalls die Ordnung 2 haben. Die einzige Matrix mit dieser Eigenschaft ist aber die negative Einheitsmatrix $-E$. (Denn die Eigenwerte von $S$ sind $\pm 1$, das Produkt der Eigenwerte ist gleich $+1$.) Diese Matrix liegt aber im Zentrum von $SU(2)$. Daraus folgt, dass $s$ im Zentrum von $G$ liegt, also ist $\{1, s\}$ ein nicht-trivialer Normalteiler von $G$, Widerspruch! Also muss eine nicht-triviale Darstellung von $G$ mindestens den Grad 3 haben.

**8.7. Satz.** *Sei $G$ eine Gruppe der Ordnung $p^2$, $p$ prim. Dann ist $G$ abelsch.*

*Beweis.* Angenommen, $G$ ist nicht abelsch. Dann besitzt $G$ eine irreduzible Darstellung von einem Grad $n > 1$. Da $G$ zumindest noch die triviale Eins-Darstellung besitzt, folgt

$$1^2 + n^2 \le p.$$

Da aber $n$ die Gruppenordnung teilt, muss $n = p$ oder $n = p^2$ sein. Beides ist mit der obigen Ungleichung nicht verträglich.