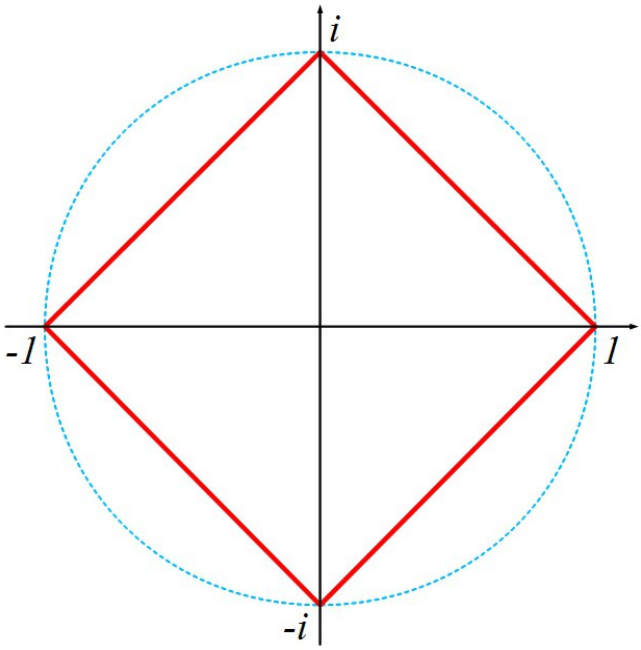
Proseminar Körpertheorie

Vortrag 9

Konstruierbarkeit des *n*-Ecks



Dennis Petersen-Endrulat

27.06.2013

Prof. Dr. K. Wingberg, K. Hübner

9.1 2-Gruppen

Proposition 9.1.1 *Sei $z\in\mathbb{C}$ konstruierbar (aus {0,1}). Dann sind auch alle Konjugierten von z konstruierbar.*

Beweis Sei $\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_n$ eine Kette von quadratischen Erweiterungen mit $z\in K_n$, sei $\mathbb{Q}\subset L$ eine Galoiserweiterung, sodass $K_n\subset L$, und sei z' eine Konjugierte von z. Dann existiert nach Satz 6.2.3 ein $\sigma\in Gal(L/\mathbb{Q})$, sodass $\sigma(z)=z'$. Setze nun $K'_j:=\sigma(K_j)$, $0\le j\le n$ (insbesondere gilt also $K'_0=\mathbb{Q}$). Dann gilt: $K'_j\subset L$ Teilkörper, $K'_{j-1}\subset K'_j$ und $[K'_j:K'_{j-1}]=2$. Nach Wantzel ist $z'\in K'_n$ somit konstruierbar.

Lemma 9.1.2 *Sei G eine endliche Gruppe mit $\#G=p^n$, $n\in\mathbb{N}$, p Primzahl. Dann gibt es eine normale Kette $\{1\}=G_0\subset G_1\subset\ldots\subset G_n=G$ mit $(G_j:G_{j-1})=p$.*

Beweis Nach 8.3 ist das Zentrum Z von G eine nichttriviale Untergruppe von G. Sei $g\in Z\setminus\{1\}$. Da $ord(g)|\#Z$, gilt $ord(g)=p^a, a\in\mathbb{N}$. Setze nun $h:=g^{p^{a-1}}\in Z$ mit $ord(h)=p$.
Sei $G_1:=<h>\subset Z\subset G$. Dann ist G_1 eine normale Untergruppe der Ordnung p von G, da jedes Element aus Z mit allen Elementen von G kommutiert. Somit gilt $\#G/G_1=p^{n-1}$.
Es folgt Induktion über n. Für n=1 ist die Behauptung klar.
Sei für n>1 eine normale Kette $\{1\}=H_0\subset H_1\subset\ldots\subset H_{n-1}=G/G_1$ mit $(H_j:H_{j-1})=p, 1\le j\le n-1$, gegeben. Betrachte nun für die surjektive kanonische Abbildung $\pi:G\to G/G_1, g\to gG_1$ das Urbild $G_j:=\pi^{-1}(H_{j-1})$. Dies ergibt eine normale Kette $G_1\subset G_2\subset\ldots\subset G_n$. Aus dem Homomorphiesatz folgt: $G_j/G_1\cong H_{j-1}$. Nach dem 2. Isomorphiesatz gilt dann:
$G_j/G_{j-1}\cong (G_j/G_1)/(G_{j-1}/G_1)\cong H_{j-1}/H_{j-2}$ => $(G_j:G_{j-1})=p\quad\forall j\le n$.
Außerdem gilt $\pi(G)=G/G_1=H_{n-1}$, also $G_n=G$.

Satz 9.1.3 *Sei $z\in\mathbb{C}$ algebraisch. Dann ist z genau dann konstruierbar, wenn der Grad der Erweiterung von $\mathbb{Q}$ erzeugt von z und dessen Konjugierten eine Potenz von 2 ist.*

Beweis Sei L die Erweiterung von $\mathbb{Q}$ erzeugt von z und dessen Konjugierten. Da $char(\mathbb{Q})=0$ ist das Minimalpolynom von z nach Lemma 9.1.4 separabel.
$\Rightarrow$ Sei $z\in\mathbb{C}$ konstruierbar. Dann ist nach Proposition 9.1.1 und Satz 1.2 jedes Element aus L konstruierbar. Da L separabel ist, existiert nach dem Satz vom primitiven Element ein $\alpha\in L$ mit $L=\mathbb{Q}[\alpha]$. Da α konstruierbar ist, ist dessen Grad eine Potenz von 2 (Folgerung 3.4) und somit auch $[L:\mathbb{Q}]$.
$\Leftarrow$ Sei $[L:\mathbb{Q}]$ eine Potenz von 2. Da L der Zerfällungskörper eines separablen Polynoms ist, ist L nach Satz 6.1.1 eine Galoiserweiterung. Sei G:=Gal(L/K), dann ist #G eine Potenz von 2. Nach Lemma 9.1.2 existiert eine Kette von Gruppen $\{1\}=G_0\subset G_1\subset\ldots\subset G_n=G$ mit $(G_j:G_{j-1})=2$.
Nach Satz 6.1.3 korrespondieren diese mit einer Kette von Erweiterungen von $\mathbb{Q}$:
$\mathbb{Q}=L^G\subset L^{G_{n-1}}\subset\ldots\subset L^{G_0}$, wobei $[L^{G_j}:L^{G_{j+1}}]=(G_{j+1}:G_j)=2$.
Somit ist jedes Element aus L – insbesondere z – konstruierbar (Wantzels Satz).

Lemma 9.1.4 *Sei K ein Körper mit char(K)=0. Dann ist jedes irreduzible Polynom $P\in K[X]$ separabel.*

Beweis Sei $P\in K[X]$ irreduzibel. Betrachte das Monom aX^n, wobei n=deg(P), $a\neq 0$ der höchste Koeffizient von P. Das Monom höchsten Grades von P' ist dann naX^{n-1}, wobei $na\neq 0$, da char(K)=0. Da P irreduzibel, deg(P')<deg(P) (also $P\neq P'$) und $P'\neq 0$ ist P nach Lemma 5.1.5 separabel.

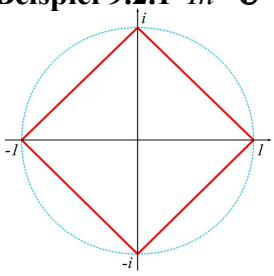
9.2 Kreisteilungserweiterungen

Definition 9.2.1 *Sei K ein Körper. Man bezeichnet die Nullstellen des Polynoms* $X^n-1\in K[X]$ *(also die Lösungen der Gleichung* $X^n=1$ *im Zerfällungskörper des Polynoms* X^n-1*) als n-te Einheitswurzeln.*

Lemma 9.2.1 *Sei K ein Körper,* $n\in\mathbb{N}$ *mit* $char(K)\nmid n$. *Dann bildet die Menge der n-ten Einheitswurzeln mit der Multiplikation eine zyklische Gruppe der Ordnung n.*

Beweis Sei $P:=X^n-1$, E bezeichne die Menge der *n*-ten Einheitswurzeln. Für n=1 ist P trivialerweise separabel. Für n>1 gilt: $P'=nX^{n-1}\neq 0$, da $char(K)\nmid n$. Da P und P' verschiedene Nullstellen besitzen, sind sie somit teilerfremd und P ist separabel. Also gilt ord(E)=deg(P)=n. Seien $\zeta,\theta\in E$. Dann gilt: $(\zeta\theta)^n=\zeta^n\theta^n=1$, $(\zeta^{-1})^n=(\zeta^n)^{-1}=1$. Assoziativität und die $1=\zeta^0$ vererben sich aus der multiplikativen Gruppe von K. Somit bildet E mit der eingeschränkten Multiplikation aus K eine Gruppe der Ordnung n. Da endliche Untergruppen der multiplikativen Gruppe eines Körpers zyklisch sind, ist somit auch E zyklisch.

Beispiel 9.2.1 *In* $\mathbb{C}$ *sind die n-ten Einheitswurzeln in der Gauß'schen Zahlenebene genau die Ecken des regelmäßigen n-Ecks im Einheitskreis, wobei eine der Ecken die 1 ist. Sie lassen sich als* $\exp(2\pi ik/n), k\in\{0,\dots,n-1\}$ *schreiben. So sind die 4-ten Einheitswurzeln in* $\mathbb{C}$ *die Ecken des regelmäßigen 4-Ecks im Einheitskreis, also* $1,i,-1$ *und* $-i$. *Außerdem gilt:* $\exp(2\pi i\cdot 0/4)=1$, $\exp(2\pi i\cdot 1/4)=i$, $\exp(2\pi i\cdot 2/4)=-1$, $\exp(2\pi i\cdot 3/4)=-i$.



Satz 9.2.2 *Sei K ein Körper,* $n\in\mathbb{N}$, *wobei* $char(K)\nmid n$. *Sei* $K\subset L$ *der Zerfällungskörper des Polynoms* X^n-1. *Dann ist L eine Galoiserweiterung und es existiert ein kanonischer injektiver Gruppenhomomorphismus* $\varphi: Gal(L/K)\to(\mathbb{Z}/n\mathbb{Z})^x=\{\bar{a}\in\mathbb{Z}/n\mathbb{Z}\mid ggT(a,n)=1\}$, *sodass für jede n-te Einheitswurzel* $\zeta\in L$ *und jedes* $\sigma\in Gal(L/K)$ *gilt:* $\sigma(\zeta)=\zeta^{\varphi(\sigma)}$. *Insbesondere ist Gal(L/K) isomorph zu* $(\mathbb{Z}/n\mathbb{Z})^x$.

Beweis Sei ζ eine primitive *n*-te Einheitswurzel. Da X^n-1 separabel ist ($\mathrm{char}(\mathbb{C})=0$, also bildet die Menge der *n*-ten Einheitswurzeln eine zyklische Gruppe der Ordnung n, Lemma 9.2.1), ist $K\subset L$ galoissch (Satz 6.1.1). Die Nullstellen des Polynoms sind genau die $\zeta^m, 0\le m\le n-1$. Sei $\sigma\in\mathrm{Gal}(L/K)$. Dann gilt $\sigma(\zeta)=\zeta^m, m\in\{0,\dots,n-1\}$. $\sigma(\zeta)$ ist eine primitive Wurzel, denn: $\sigma(\{\zeta^k\mid k\in\{0,\dots,n-1\}\})=\{\zeta^k\mid k\in\{0,\dots,n-1\}\}$ und $\sigma(\zeta^k)=\sigma(\zeta)^k\ \forall k\in\{0,\dots,n-1\}$.
Gilt $\sigma(\zeta)^k=1$, so folgt $\zeta^k=1$, da $\sigma(\zeta)$ eine primitive Wurzel ist. Somit ist m teilerfremd zu n. Es lässt sich folglich eine Abbildung $\varphi:\mathrm{Gal}(L/K)\to(\mathbb{Z}/n\mathbb{Z})^x$ definieren.
Sei θ eine beliebige *n*-te Einheitswurzel und $a\in\{0,\dots,n-1\}$, sodass $\theta=\zeta^a$. Dann gilt: $\sigma(\theta)=\sigma(\zeta^a)=\sigma(\zeta)^a=(\zeta^m)^a=(\zeta^a)^m=\theta^m$, also $\sigma(\theta)=\theta^{\varphi(\sigma)}$
φ ist somit unabhängig von der Wahl der primitiven Wurzel ζ. Seien nun $\sigma,\tau\in\mathrm{Gal}(L/K)$ mit $\sigma(\zeta)=\zeta^m, \tau(\zeta)=\zeta^k$. Dann gilt: $(\sigma\circ\tau)(\zeta)=\sigma(\zeta^k)=\zeta^{km}\Rightarrow\varphi(\sigma\circ\tau)=\varphi(\sigma)\varphi(\tau)$, also ist φ ein Gruppenhomomorphismus. Sei $\varphi(\sigma)=1$, dann gilt $\sigma(\theta)=\theta$. Es folgt $\sigma=\mathrm{id}$ und somit φ injektiv, da φ einen trivialen Kern besitzt.

9.3 Konstruierbarkeit eines regelmäßigen *n*-Ecks

Definition 9.3.1 *Eine Fermatsche Primzahl ist eine Primzahl der Form* $F_m = 2^{2^m}+1, m\in\mathbb{N}_0$. *Bisher sind nur* $F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65.537$ *als Fermatsche Primzahlen bekannt.*

Satz 9.3.2 *Ein regelmäßiges n-Eck ist genau dann konstruierbar, wenn n das Produkt einer Potenz von 2 und paarweise verschiedenen Fermatschen Primzahlen ist.*

Beweis Sei $P\subset\mathbb{N}\setminus\{1,2\}$, sodass das regelmäßige *n*-Eck für alle $n\in P$ konstruierbar ist. Nach Proposition 9.1.1 gilt für $n\geq 3$: $n\in P \Leftrightarrow \exp(2\pi i/n)$ konstruierbar. Der Beweis erfolgt über die folgenden Lemmata a) – e) :

a) $n\in P\Rightarrow 2n\in P$
Sei ein regelmäßiges *n*-Eck bereits konstruiert. Konstruiert man nun eine Gerade durch den Mittelpunkt der Strecke zwischen je zwei nebeneinander liegenden Ecken A und B und den Ursprung O, so teilt diese den Winkel $\widehat{AOB}$ in zwei gleiche Teile.

b) $n\in P\Rightarrow \forall m\in\mathbb{N}, m\geq 3, m|n:\ m\in P$
Verbinde jede (n/m)-te Ecke, um ein regelmäßiges m-Eck zu konstruieren.

c) $m, n\in P$ *teilerfremd* $\Rightarrow mn\in P$
Seien $m,n\in P$ teilerfremd. Dann gilt ggT(m,n)=1 und nach dem Lemma von Bézout existieren dann $u,v\in\mathbb{Z}$ für die gilt: $um+vn=1\Leftrightarrow u/n+v/m=1/mn$
$\Rightarrow \exp(2\pi i/mn)=\exp(2\pi i(u/n+v/m))=(\exp(2\pi i/n))^u(\exp(2\pi i/m))^v\Rightarrow mn\in P$

a) zeigt, dass Potenzen von 2 konstruierbar sind, b), dass man die Konstruierbarkeit eines n-Ecks auf die Primfaktoren von n zurückführen kann, und aus c) folgt,dass das Produkt von paarweise verschiedenen Primzahlen aus P (sowie von Potenzen von 2) auch in P liegt. Es bleibt also noch zu zeigen,dass P nur Fermatsche Primzahlen enthält und dass das Quadrat einer Primzahl aus P nicht in P liegt, die ungeraden Primfaktoren jedes $n\in P$ also die Vielfachheit 1 haben.
Sei $p\in\mathbb{N}\setminus\{1,2\}$ im Folgenden also eine Primzahl.

d) $\exp(2\pi i/p)\in\mathbb{C}$ *ist algebraisch über* $\mathbb{Q}$ *und hat den Grad p-1. Die Erweiterung von* $\mathbb{Q}$ *erzeugt durch die p-ten Einheitswurzeln hat ebenfalls den Grad p-1.*
Sei M das Minimalpolynom von $\exp(2\pi i/p)$. Dann ist M normiert mit ganzzahligen Koeffizienten und teilt $(X^p-1)/(X-1)=1+X+...+X^{p-1}$, also $\exists Q\in\mathbb{Z}[X]$:
$(X^p-1)/(X-1)=M(X)Q(X)$. Sei a:=deg(M), b:=deg(Q). Dann gilt $a+b=p-1$ und $a\geq 2$, da $\exp(2\pi i/p)\notin\mathbb{Q}$. Modulo p gilt: $X^p-1\equiv(X-1)^p$ (Binomischer Lehrsatz)
Durch Eindeutigkeit der Zerlegung in irreduzible Faktoren über $\mathbb{Z}/p\mathbb{Z}$ gibt es $A,B\in\mathbb{Z}[X]$:
$M=(X-1)^a+pA(X),\ Q=(X-1)^b+pB(X)$
$\Rightarrow (X^p-1)/(X-1)=M(X)Q(X)=(X-1)^{a+b}+p(A(X)(X-1)^b+B(X)(X-1)^a)+p^2A(X)B(X)$
Setze nun X:=1. Angenommen, $b\geq 1$, dann folgt $p=p^2AB(1)$. Widerspruch da $AB(1)\in\mathbb{Z}$!
$\Rightarrow b=0$, also $a=p-1\Rightarrow$ Grad von $\exp(2\pi i/p)$ über $\mathbb{Q}$ gleich $p-1$. Da $\exp(2\pi i/p)$ den Zerfällungskörper von X^n-1 über $\mathbb{Q}$ erzeugt, folgt die zweite Behauptung.

Nach Satz 9.1.3 ist $\exp(2\pi i/p)$ genau dann konstruierbar, wenn $p-1$ eine Potenz von 2 ist, wenn also gilt: $p=2^n+1,\ n\in\mathbb{N}$. Nach Lemma 9.3.3 ist p dann auch eine Fermatsche Primzahl.

e) $\exp(2\pi i/p^2)\in\mathbb{C}$ *ist algebraisch mit dem Grad p(p-1) über* $\mathbb{Q}$.
Dieser Beweis erfolgt analog zu d):
$\exp(2\pi i/p^2)$ ist keine Nullstelle von X^p-1, betrachte also das Polynom $(X^{p^2}-1)/(X^p-1)$:
Sei $M\in\mathbb{Z}[X]$ das Minimalpolynom von $\exp(2\pi i/p^2)$, dann existiert ein $Q\in\mathbb{Z}[X]$, sodass $(X^{p^2}-1)/(X^p-1)=M(X)Q(X)$. Da $X^{p^2}-1\equiv(X-1)^{p^2}$ modulo p, existieren $A,B\in\mathbb{Z}[X]$ mit $M=(X-1)^a+pA(X)$, $Q=(X-1)^b+pB(X)$, $a:=\deg(M)\geq 2$, $b:=\deg(Q)$. Somit gilt:
$(X^{p^2}-1)/(X^p-1)=(X-1)^{p^2-p}+p((X-1)^aB(X)+(X-1)^bA(X))+p^2A(X)B(X)$
Mit $X:=1$ folgt dann b=0 und somit $a=p^2-p$.

Da $p(p-1)$ von p geteilt wird, kann $p(p-1)$ keine Potenz von 2 sein und somit ist $\exp(2\pi i/p^2)$ nicht konstruierbar. Das Quadrat einer Primzahl aus P ist also nicht in P enthalten.

Lemma 9.3.3 $2^n+1, n\in\mathbb{N}$ *prim* $\Rightarrow$ $n=2^m, m\in\mathbb{N}_0$

Beweis Für n=1 wähle m:=0, für n=2 wähle m:=1.
Sei $n\geq 3$. Angenommen, 2^n+1 sei prim mit $n\neq 2^m\ \forall m\in\mathbb{N}_0$. $\Rightarrow$ $n=ab, 1\leq a<n, 1<b\leq n$, b ungerade. Dann gilt: $2^n+1=(2^a)^b+1\equiv(-1)^b+1$ modulo $2^a+1=0$ $\Rightarrow$ $2^a+1|2^n+1$.
Widerspruch zu 2^n+1 prim!

Literatur

Chambert-Loir, Antoine: A Field Guide to Algebra, Springer 2005