Algebra 1 WS 22/23
LMU München

Markus Land

Grundmotivation:

Sei $ax^2 + bx + c = 0$ $(a \neq 0)$ $\circledast$ eine quadr. Gleichung.

Wir lernen in der Schule, dass man folgende allgemeine Lösungsformel für $\circledast$ hat:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ziel dieser Vorlesung ist, zu beweisen dass es für Polynomgleichungen vom Grad ≥ 5 (also $p(x) = ax^n + \dots$ mit $a \neq 0$, $n \geq 5$) keine solche allgemeine Lösungsformel gibt.

Als Methoden führen wir spezielle algebraischen Körpererweiterungen ein [Galoiserweiterungen], zeigen dann das allg. Lösungsformeln mit noch spezielleren Körperer. zu tun haben [Radikalerweiterungen] und zeigen dann mit Hilfe von Gruppentheorie, dass allg. Galoiserweiterungen nicht durch iterierte Radikalerweiterungen gegeben sind.

§ Elementare Gruppentheorie

Sei M eine Menge. Eine binäre Verknüpfung auf M ist eine Abbildung $\star : M \times M \longrightarrow M$, geschrieben $a \star b$ oder ab statt $\star(a,b)$.

Eine binäre Verknüpfung $\star$ ist

- assoziativ, falls $\forall a,b,c \in M$ gilt, dass $(a \star b) \star c = a \star (b \star c)$
- kommutativ, falls $\forall a,b \in M$ gilt, dass $a \star b = b \star a$ (manchmal auch abelsch)

Definition 1.1 Ein Monoid besteht aus einem Tripel $(M, *, e)$ wobei
- M eine Menge,
- $*$ eine assoziative binäre Verknüpfung auf M
- $e \in M$ ein element, sodass $\forall a \in M$ gilt $a * e = a = e * a$.
  (e heißt ein neutrales Element bzgl. $*$)

ein Monoid $(M, *, e)$ heißt • kommutativ/abelsch falls $*$ kommutativ ist
ein Monoid ist eine **Gruppe**, falls $\forall a \in M$ ein $b \in M$ existiert
sodass $a * b = e = b * a$. (b heißt ein inverses zu a)

Bemerkung: • ein neutrales element ist, so es existiert, eindeutig.
• inverse sind, so sie existieren, eindeutig:

In der Tat: • seien $e, e' \in M$ neutral bzgl $*$. Dann gilt

$$e = e * e' = e'$$
(e' neutral, e neutral.)

• seien b, b' inverse zu a. Dann gilt

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$$

Wir schreiben dann a^{-1} für den eindeutige inverse zu a (so es existiert).

Bemerkung: für eine abelsche Gruppe schreiben wir oft $+$ statt $*$ und $(-a)$ statt a^{-1}, und 0 statt e

Konstruktion: Sei $(M, *, e)$ ein Monoid. Dann setzen wir
$(M, *, e)^{op} = (M, *^{op}, e)$ mit $a *^{op} b := b * a$.
• $(M, *, e)^{op}$ ist wieder ein Monoid.
• $(M, *, e)$ ist eine Gruppe $\Leftrightarrow$ $(M, *, e)^{op}$ ist eine Gruppe
• $(M, *, e) = (M, *, e)^{op}$ $\Leftrightarrow$ M ist kommutativ

Beispiele 1.2 a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ bzgl addition. Jeder Körper / VR sind Gruppen hat (per definition) eine zugrunde liegende abelsche Gruppe.

b) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ bzgl multiplikation, 1 [redacted]

c) $\mathbb{Z}\cdot\{0\}$, $\mathbb{Q}\cdot\{0\}$, $\mathbb{R}\cdot\{0\}$, $\mathbb{C}\cdot\{0\}$ bzgl multiplikation sind monoide (gruppen außer im ersten Fall)

d) $\mathbb{R}_{>0}$ bzgl multiplikation

e) für K ein Körper · $M_n(K)$ bzgl. matrix multiplikation (monoid)
· $GL_n(K)$ —"— (gruppe)
· $SL_n(K)$ —"— (—"—)

d) $\left(\{V \text{ ein } K\text{-VR}\}/_{\text{isom}}, \oplus, 0\right)$ ab. Monoid. (K ein Körper) (endl. dim)

e) M eine Menge, $S(M) = \{f: M \to M \text{ bijektiv}\}$
dann ist $(S(M), \circ, id_M)$ eine Gruppe.

f) M Menge, G Gruppe/Monoid. $\mathrm{Hom}(M,G) := \{f: M \to G\}$. betrachte
$(\mathrm{Hom}(M,G), *, e)$ mit · $(f * f')(m) = f(m) * f'(m)$
· $e(m) = e$
eine Gruppe/Monoid.
Sei $\mathrm{Hom}_{\text{endl}}(M,G) \subseteq \mathrm{Hom}(M,G)$ die Abb. $f: M \to G$ s.d.
$f(m) = e$ für fast alle $m \in M$ (d.h. alle bis auf endl. viele)
dann ist $\mathrm{Hom}_{\text{endl}}(M,G)$ ein Untermonoid (d.h. eine Teilmenge welches das neutrale Element enthält und bzg das produkt (die binäre Verknüpfung) zweier Elemente aus der Teilmenge wieder in der Teilmenge lebt). siehe Def 1.3

g) Sei X eine Menge und $\forall x \in X$ sei M_x ein Monoid. Dann ist $\prod_{x \in X} M_x$ ein Monoid vermöge: $(m_x)_{x\in X} * (m'_x)_{x\in X} = (m_x * m'_x)_{x\in X}$ und $e = (e_x)_{x\in X}$ ($(M_x, *, e_x)$)
sind alle M_x gruppen so ist auch $\prod M_x$ eine Gruppe

Definition 13 Sei G ein Monoid. Eine Teilmenge $H \subseteq G$ heißt Untermonoid, falls $e \in H$ und $\forall a,b \in H$ gilt $a \cdot b \in H$.
Ist G eine Gruppe so heißt ein Untermonoid $H \subseteq G$ Untergruppe falls $\forall a \in H$ gilt, dass $a^{-1} \in H$.

Konstruktion: Sei M ein Monoid. Dann ist
$M^\times := G = \{ m \in M \mid \exists \text{ Inverses zu } m \} \subseteq M$ ein Untermonoid.
Des weiteren ist $M^\times$ eine Gruppe, die größte Untergruppe von M.

Beweis:
- $e \in G$ ✓
- Seien $m, m' \in M$ zz: $m \cdot m' \in M$. Seien dafür $a, a' \in M$ Inverse. Dann gilt $(mm') \cdot (a'a) = m(m'a')a = mea = ma = e$ und $(a'a)(mm') = e$ analog.
- offenbar ist G eine Gruppe und die größte die in M enthalten ist. ∎

Beispiele 1.4 a) G Gruppe, so ist G und $\{e\}$ jeweils eine UG.
b) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ sind UG bzgl $+$
c) $\mathbb{Z} \setminus \{0\} \subseteq \mathbb{Q} \setminus \{0\} \subseteq \mathbb{R} \setminus \{0\}$ sind UM / UG bzgl. $\cdot$
d) $\mathbb{Q} \setminus \{0\} = \mathbb{Q}^\times$, $\mathbb{R} \setminus \{0\} = \mathbb{R}^\times$ (bzgl. $\cdot$) (dies ist eine der definierenden Eigenschaften von (schief)körpern)
e) $m \in \mathbb{Z}$ so ist $m\mathbb{Z} = \{ m \cdot n \mid n \in \mathbb{Z} \}$ eine UG bzgl $+$
(wir zeigen später dass alle UG von $(\mathbb{Z}, +, 0)$ so aussehen)
f) G Gruppe, $g \in G$, $\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \} \subseteq G$ eine UG

Notation: Wir sagen eine Gruppe G heißt zyklisch falls es ein Element $g \in G$ gibt, sodass $\langle g \rangle = G$.

Definition 1.5 G, G' Monoide. Eine Abbildung $\varphi: G \to G'$ heißt Monoidhomomorphismus falls

- $\varphi(e) = e'$ $(e \in G,\ e' \in G'$ die neutr. elemente)
- für alle $a, b \in G$ gilt $\varphi(ab) = \varphi(a)\varphi(b)$.

Sind G, G' gruppen so nennen wir Monoidhom. auch Gruppenhom.

ÜA: φ Gruppenhom $\iff \left[\forall a,b \in G \quad \varphi(ab) = \varphi(a)\varphi(b)\right]$ und es gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$

Ein Monoidhom. $\varphi: G \to G'$ heißt Isomorphismus falls φ bijektiv ist

(äquiv. $\exists\, \psi: G' \to G$ monoidhom. sd $\varphi\psi = id_{G'}$ und $\psi\varphi = id_G$)

Ein Monoidhom. $G \to G$ heißt endomorphismus, ein endomorphismus welcher ein Isomorphismus ist automorphismus.

ÜA: $\varphi: G \to G'$ monoidhom. wir setzen

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e'\}$$
$$\mathrm{Im}(\varphi) = \{\varphi(g) \mid g \in G\}$$

Dann sind $\ker(\varphi) \leq G$ und $\mathrm{Im}(\varphi) \leq G'$ Untermonoide

(Untergruppen falls G, G' Gruppen)

ÜA: Ein Gruppenhom φ ist injektiv $\iff \ker(\varphi) = \{e\}$

gilt dies auch für Monoidhomomorphismen?

Beispiele 1.6 a) $\mathrm{Hom}_{Mon}(\mathbb{N}, M) = \{f: \mathbb{N} \to M \mid \text{Monoidhom}\}$

dann ist $\mathrm{Hom}_{Mon}(\mathbb{N}, M) \xrightarrow{ev_1} M$ eine bijektion

$f \longmapsto f(1)$

a') $\mathrm{Hom}_{Grp}(\mathbb{Z}, G) = \{f: \mathbb{Z} \to G \mid \text{Gruppenhom.}\}$

$\mathrm{Hom}_{Grp}(\mathbb{Z}, G) \xrightarrow{ev_1} G$ eine bijektion

b) Sei G Gruppe, M Monoid $\varphi: G \to M$ Gruppe Monoidhom.

so faktorisiert φ als $\bar{\varphi}: G \to M^\times \leq M$, $\bar{\varphi}$ Gruppenhom.

Wir haben also $\mathrm{Hom}_{\mathrm{Grp}}(G, M^\times) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Mon}}(G, M)$

c) Sei G eine Gruppe. Betrachte die Abbildung

$G \longrightarrow S(G) = \mathrm{Hom}_{\mathrm{Mengen}}(G,G)^\times$

$g \longmapsto (h \xmapsto{l_g} g \cdot h)$ dies ist ein injektiver Gruppenhom.

(ÜA: gilt selbiges für Monoide statt Gruppen?)

Jede Gruppe "ist" also Untergruppe einer "Permutationsgruppe".

und jede endl. Gruppe eine Untergruppe von $S_n = S(\{1,\dots,n\})$

d) $G \longrightarrow S(G)$ $\quad g \longmapsto (c_g : h \mapsto ghg^{-1})$ ist dies ein injektiver Gruppenhom?

$\quad \rightsquigarrow \mathrm{Aut}(G)$

ÜA bestimme den Kern von $g \mapsto c_g$ (den Zentrum von G)

e) G Gruppe: ist $G \longrightarrow G$, $g \longmapsto g^n$ für $n \in \mathbb{N}$ ein Gruppenhomomorphismus?

(Ja, falls G abelsch oder $n = 0$)

Nebenklassen, Normalteiler, Quotienten

Sei G eine Gruppe, $H \leq G$ eine Untergruppe. Eine Linksnebenklasse von H in G ist eine Teilmenge von G von der Form

$aH = \{ah \mid h \in H\}$, $a \in G$. Wir schreiben G/H für die Menge der H-Linksnebenklassen.

Lemma 1.7 • Je zwei H-Linksnebenklassen haben eine Bijektion zwischeneinander

• Je zwei H-Linksnebenklassen sind gleich oder disjunkt

• $G = \coprod_{a \in G/H} aH$ eine disjunkte Zerlegung.

Bew: Sei $a \in G$ und aH die Linksnebenklasse. Dann hat man die Abbildung $H \longrightarrow aH$, $h \mapsto ah$. Diese ist per def. surjektiv und (injektiv: $ah = ah' \Rightarrow h = h'$)

da $a \in G$ beliebig folgt der erste Teil.

Als zweites nehmen wir an, dass $aH \cap bH \neq \emptyset$

Sei also $ah = bh'$ für $h, h' \in H$. Dann gilt $b^{-1}a = h'h^{-1} \in H$

$\Rightarrow bH = b(b^{-1}aH) = aH$. Für das letzte reicht es zu sehen dass für $g \in G$ beliebig $g \in gH$.

Bemerkung: Sei $H \leq G$ eine Untergruppe. Wir definieren eine Äquivalenzrelation $\sim_H$ auf G indem:

$$g \sim_H g' \iff (g')^{-1} \cdot g \in H \quad | \text{ (Übung: dies ist eine äquiv. relation)}$$

Dann gilt $g \sim_H g' \iff gH = g'H$.

Die Menge G/H der H-Linksnebenklassen ist also die Menge der Äquivalenzklassen von $\sim_H$.

Analog gibt es Rechtsnebenklassen Hg. Die Abbildung $G \xrightarrow{(\cdot)^{-1}} G$, $g \mapsto g^{-1}$ schickt gH auf Hg^{-1} und $G/H \to H\backslash G$, $gH \mapsto Hg^{-1}$ ist eine Bijektion. $= \{Hg \mid g \in G\}$

Für $H \leq G$ ist der **Index von H in G** gegeben durch

$$[H:G] = |G/H| = |H\backslash G|$$

Proposition 1.8 (Satz von Lagrange) Ist G eine endliche Gruppe, so gilt $|G| = |H| \cdot [H:G]$. Insbesondere teilt $|H|$ $|G|$.

Beweis: Nach Lemma 1.7 gilt

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |G/H| \cdot |H| = [H:G] \cdot |H| \qquad \square$$

Bemerkung Versuchen wir mal auf G/H, der Menge der H-Linksnebenkl., eine Monoidstruktur zu bauen, derart, dass die kan. Abbildung $G \to G/H$, $g \mapsto gH$ ein Monoidhom. ist. Dann muss gelten

$$gH * g'H = (g \cdot g')H \quad \text{und} \quad eH = H \text{ muss das neutr. Elem. sein.}$$

um Wohldefiniertheit zu prüfen, seien $g_0 \sim_H g_1$, also $g_1^{-1} g_0 \in H$

Dann gilt $g_0 g'H = g_0 H * g'H = g_1 H * g'H = g_1 g'H$.

Dies ist der Fall gdw $g'^{-1} \underbrace{(g_1^{-1} g_0)}_{\in H} g' \in H$

dies muss nicht immer der Fall sein (siehe Bsp 1.10)

Definition 1.9 Eine UG $H \leq G$ heißt Normalteiler, falls für alle $g \in G$ gilt, dass $gHg^{-1} \in H$ ($\Leftrightarrow gH = Hg$). Wir schreiben dann $H \trianglelefteq G$.

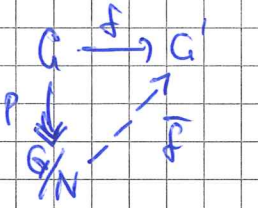
Beispiele 1.10
- $e, G \trianglelefteq G$ sind NT
- ist G abelsch, $H \leq G$ so ist H NT
- sei $G = S_3 = S(\{1,2,3\})$ und $\tau_{1,2}, \tau_{1,3}$ die Transpositionen $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$. Dann gilt $\tau_{1,3}^{-1} = \tau_{1,3}$ und $\tau_{1,3} \circ \tau_{1,2} \circ \tau_{1,3} = \tau_{2,3}$. Da $\tau_{2,3} \notin \{e, \tau_{1,2}\} \overset{\text{UG}}{\subseteq} S_3$ folgt, dass $\{e, \tau_{1,2}\}$ kein NT ist.

Lemma 1.11 Ist $H \trianglelefteq G$ ein NT, so wird G/H vermöge der obigen Konstruktion eine Gruppe und $G \xrightarrow{p} G/H$ ein Gruppenhomomorphismus mit $\ker(p) = H$. Ist allgemein $f: G \to G'$ ein Gruppenhomom. so ist $\ker(f) \subseteq G$ ein NT.

Beweis: Wie angedeutet ist die multpl. $gH * g'H = gg'H$ wohldef. da $H \trianglelefteq G$. Unitalität und Assoziativität sind dann offenbar, und auch, dass p ein Gruppenhom. ist. (*) Für letzteres, sei $g \in G$ und $k \in \ker(f)$. dann gilt $f(gkg^{-1}) = f(g) \cdot f(k) \cdot f(g^{-1}) = f(g) \cdot e \cdot f(g)^{-1} = e$, und somit $gkg^{-1} \in \ker(f)$, also $\ker(f) \trianglelefteq G$. ∎

(*) $\ker(p) = \{g \in G \mid gH = H\} = \{g \in G \mid g \sim_H e \Leftrightarrow g \in H\}$

Satz 1.12 (Homomorphiesatz) Sei $f: G \to G'$ ein Gruppenhomom. und $N \trianglelefteq G$ mit $N \subseteq \ker(f)$. Dann existiert eine eind. Gruppenhom. $\bar{f}: G/N \to G'$ sodass das Diagramm



kommutiert. (d.h. dass $f = \bar{f} \circ p$)

Es gelten: $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$, $\ker(\bar{f}) \overset{(B)}{=} \mathrm{Im}(p|_{\ker(f)}) \overset{!!}{=} p(\ker(f))$; $\ker(f) \overset{(A)}{=} p^{-1}(\ker(\bar{f}))$ und $\bar{f}$ ist injektiv genau dann wenn $N = \ker(f)$ gilt.

Beweis: 1) Da p surjektiv existiert höchstens eine Abb. $\bar{f}$ mit $f = \bar{f} \circ p$. (wir müssen $\bar{f}(gN) = f(g)$ setzen).

die so definierte "Abb." $\bar{f}$ ist wohldefiniert: seien $g, g' \in G$ mit $p(g) = p(g')$. Dann gilt $g'^{-1} g \in N \subseteq \ker(f)$. Daher gilt

$$f(g') = f(g') \cdot f(g'^{-1} \cdot g) = f(g' g'^{-1} \cdot g) = f(g).$$

Per Konstruktion ist $\bar{f}$ ein Gruppenhom. $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$ folgt aus der Tatsache, dass p surjektiv ist. Wir zeigen jetzt $\ker(\bar{f}) = p^{-1}(\ker(f))$: sei $g \in G$. aus $f = \bar{f} \circ p$ folgt dass $f(g) = \bar{f}(p(g))$, somit $g \in \ker(f) \Leftrightarrow p(g) \in \ker(\bar{f})$. Dann folgt aber auch, dass

$$p(\ker(f)) = p(p^{-1}(\ker(\bar{f}))) = \ker(\bar{f}) \quad (\text{da } p \text{ surjektiv}).$$

wir wissen, dass $\bar{f}$ injektiv ist, gdw $\ker(\bar{f}) = \{e\}$.
aber $\ker(\bar{f}) = p(\ker(f))$ und $p(\ker(f)) = \{e\} \Leftrightarrow$
$\ker(f) \subseteq \ker(p) = N \subseteq \ker(f)$ ∎

Korollar 1.13 Ist $f: G \to G'$ surjektiv, so induziert f einen Isom.

$$\bar{f}: G/\ker(f) \xrightarrow{\cong} G'.$$

Ist G eine Gruppe, $H, H' \subseteq G$ Teilmengen so definieren wir

$$HH' = \{h \cdot h' \mid h \in H, h' \in H'\} \subseteq G.$$

Satz 1.14 Sei G eine Gruppe

1) [1. Isomorphiesatz] $H \subseteq G$ UG, $N \trianglelefteq G$ NT. Dann ist $HN \subseteq G$ UG, $N \trianglelefteq HN$ und $H \cap N \trianglelefteq H$ Normalteiler und die kanonische Abb.

$$H/H\cap N \xrightarrow{\cong} HN/N$$ ist ein Isom.

2) [2. Isomorphiesatz] Seien $N, H \trianglelefteq G$ NT, $N \subseteq H \subseteq G$. So ist $N \trianglelefteq H$, $H/N \trianglelefteq G/N$ und die kan. Abbildung

$$G/H \longrightarrow (G/N)/(H/N)$$ ist ein Isom.

Beweis: alle Aussagen, dass UG normalteiler sind rechnet man einfach nach. ($N \subseteq H \subseteq G$ UG, $N \trianglelefteq G \Rightarrow N \trianglelefteq H$)

betrachte dann die komm. diagramme

$$\begin{array}{ccc} H\cap N & \hookrightarrow & N \\ \downarrow & & \downarrow \\ H & \hookrightarrow & HN \\ \downarrow & & \downarrow \\ H/_{H\cap N} & \xrightarrow[\exists!]{\Phi} & HN/_N \end{array} \qquad \begin{array}{ccc} H & \twoheadrightarrow & H/_N \\ \downarrow & & \downarrow \\ G & \twoheadrightarrow & G/_N \\ \downarrow & & \downarrow \\ G/_H & \xrightarrow[\exists!]{\Psi} & (G/_N)/(H/_N) \end{array}$$

die sch. sind, dass die linken horizontalen Abb. isom. sind.

Nach Satz 1.12 sind Φ und Ψ injektiv (check)

Ψ ist per Konstruktion surjektiv, es verbleibt also zu sehen, dass Φ surj. ist

sei also $hn \in HN$. Dann gilt $h^{-1} \cdot hn = n \in N$, also $hn \sim_N h$.

Dann gilt $\Phi(h \cdot H\cap N) = h \cdot N = hn \cdot N$ und somit ist Φ auch surj. ∎

Zyklische Gruppen

Sei G eine Gruppe, $X \subseteq G$ eine Teilmenge. Dann ist

$\bigcap_{\substack{H \subseteq G \text{ UG} \\ X \subseteq H}} H$ eine UG von G, die kleinste, welche X enthält.

wir nennen sie die von X erzeugte UG und schreiben $\langle X \rangle$. Siehe Bsp. 1.4 f) für den Fall $X = \{g\}$.

Sei $H = \langle x \rangle$ eine von x erzeugte (zyklische Gruppe).

betrachten wir den Homom. $\mathbb{Z} \xrightarrow{\Phi_x} H$. Dann ist (per definition)

$1 \mapsto x$

Φ_x surjektiv. es folgt dass zyklische Gruppen abelsch sind.

Beispiele 1.15 a) $\mathbb{Z}$ ist zyklisch (unter +)

b) ist H zyklisch und $H \to H'$ surj. dann ist H' zyklisch

($\mathbb{Z} \to H \to H'$ ist surj. $\Rightarrow H'$ = erzeugt von dem Bild von $1 \in \mathbb{Z}$).

insbesondere für $0 \neq m \in \mathbb{Z}$ ist $m\mathbb{Z} = \mathrm{Im}(\cdot m : \mathbb{Z} \to \mathbb{Z})$ zyklisch.

und $m\mathbb{Z} \subseteq \mathbb{Z}$ ein NT (da $\mathbb{Z}$ abelsch). $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ zeigt, dass

$\mathbb{Z}/m\mathbb{Z}$ auch zyklisch ist.

Satz 1.16 Sei G eine zyklische Gruppe. Dann gilt

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } |G| = \infty \\ \mathbb{Z}/m\mathbb{Z} & \text{falls } |G| = m < \infty. \end{cases}$$

Beweis: da G zyklisch existiert eine Surjektion $\mathbb{Z} \xrightarrow{\varphi} G$.
Nach 1.13 bekommen wir $\mathbb{Z}/\ker(\varphi) \xrightarrow{\bar{\varphi}}_{\cong} G$.

wir zeigen nun, dass jede UG H von $\mathbb{Z}$ die Form $m\mathbb{Z}$, für $m \in \mathbb{Z}$, hat. Dann folgt der Satz sobald wir sehen, dass für $m \geq 0$ $|\mathbb{Z}/m\mathbb{Z}| = m$ ist. ($\{0, 1, \dots, m-1\}$ sind repräsentanten von $\mathbb{Z}/m\mathbb{Z}$).
sei $H \leq \mathbb{Z}$. falls $H = \{0\}$ so gilt $H = 0 \cdot \mathbb{Z}$.
ist $H \neq \{0\}$, sei $m \in H$ das kleinste positive Element (bzgl $\leq$ auf $\mathbb{Z}$ wie gewohnt)
dann folgt $m\mathbb{Z} \subseteq H$. wir behaupten, dass $m\mathbb{Z} = H$.
sei $x \in H$. dann ex ein maximales $n \in \mathbb{Z}$ sd. $nm \leq x$
obdA $x \geq 0$
($\Leftrightarrow x < (n+1) \cdot m$)
wir finden, dass $x - nm \in H \cap \mathbb{Z}_{\geq 0}$ und $(x - nm) < m$ (sonst wäre $x \geq (n+1)m$ im Widerspruch zur Maximalität von n)
dann folgt aus der Minimalität von m, dass $x - nm = 0$ und damit $x = nm$ ∎

Lemma 1.17 UG von zyklischen Gruppen sind zyklisch.

Beweis: wir haben gesehen, dass $H \subseteq \mathbb{Z}$ erfüllt, dass $H = m\mathbb{Z}$. ausserdem ist $\cdot m: \mathbb{Z} \to m\mathbb{Z}$ ein Isomorphismus. Sei $H \subseteq \mathbb{Z}/m\mathbb{Z}$ und $p: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ die kan. projektion. Dann ist $p^{-1}(H) \subseteq \mathbb{Z}$ eine UG welche $m\mathbb{Z}$ enthält.
es gilt also $p^{-1}(H) = n\mathbb{Z}$ und $m\mathbb{Z} \subseteq n\mathbb{Z}$. da $n\mathbb{Z}$ zyklisch ist folgt, dass $m = kn$ für ein k. Nach den Isomorphiesätzen gilt
$H \cong n\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$. ∎

Bem: allgemein gilt: $G \xrightarrow{\varphi} G'$ Gruppenhom mit G zyklisch $\Rightarrow$ $\mathrm{im}(\varphi)$ zyklisch und $\ker(\varphi)$ zyklisch.

Sei nun G eine Gruppe, $g \in G$ und $\langle g \rangle$ die von g erz. (zyklische) UG von G. Die Ordnung von g ist

$$\operatorname{ord}(g) := |\langle g \rangle| \quad \in \mathbb{N}_{\geq 1} \cup \{\infty\}$$

Bemerkung: $\operatorname{ord}(g)$ ist minimal (in $\mathbb{N}_{\geq 1}$) mit der Eigenschaft $g^{\operatorname{ord}(g)} = e$

Satz 1.18 (Satz von Fermat) Sei G eine endl. Gruppe und $g \in G$.
Dann gilt $\operatorname{ord}(g) \mid |G|$. Insbesondere gilt $g^{|G|} = e \quad \forall g \in G$.

Beweis: $\operatorname{ord}(g) = |\langle g \rangle|$ und $\langle g \rangle \leq G$ UG. Nach Lagrange gilt also $|\langle g \rangle| \mid |G|$. Außerdem: $g^{|G|} = \left(g^{\operatorname{ord}(g)}\right)^m = e^m = e$ für geeign. $m \in \mathbb{N}$.

Korollar 1.19 Sei G eine Gruppe mit $|G| = p$ prim. Dann ist G zyklisch.

Beweis: Sei $g \in G \setminus \{1\}$ $(p \neq 1)$. Dann gilt $\operatorname{ord}(g) = |G|$. ($\operatorname{ord}(g) \neq 1$ und $|G|$ prim)
Sei $\mathbb{Z} \to G$, $1 \mapsto g$, so bekommen wir eine induz. Surjektion $\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z} \twoheadrightarrow G$, beide Mengen haben $\operatorname{ord}(g)$ viele Elemente. ∎