LAII 2002 (Hiß)

Alexander Langer <alex@big.endian.de>
Wer dieses Skript vervollständigen möchte, findet die Sourcen auf www.s-inf.de

22. Juli 2002

Literatur

1. Liste auf http://www.math.rwth-aachen.de/LAII2002/

2. Lorenz, Lineare Algebra II

3. Lüneburg, Vorlesungen über LA

1 Einleitendes

1.1 Def. und Bemerkung

Sei $(A,+)$ abelsche Gruppe, $U \leq A$
$A/U := \{a+U | a \in A\}$
heißt Menge der **Restklassen von A modulo U**.
Durch die Verknüpfung
$+ : A/U \times A/U \to A/U$, $(a+U)+(b+U) = (a+b)+U$ wird A/U zu einer abelschen Gruppe.
Die kanonische Abbildung $\pi : A \to a/U, a \to a+U$ ist surjektiver Gruppenhomomorphismus.

Beweis:

+ ist wohldefiniert, d.h. repräsentantenunabhängig.
$a+U = a'+U$, $b+U = b'+U$
$\Rightarrow a-a' \in U, b-b' \in U$
$\Rightarrow (a+b)-(a'+b') \in U$
$\Rightarrow (a+b)+U = (a'+b')+U$
$\pi(a+b) = (a+b)+U = (a+U)+(b+U) = \pi(a)+\pi(b)$
A/U heißt **Faktorgruppe** von A modulo U.

1.2 Satz

(a) Sei A eine endlische abelsche Gruppe und $U \leq A$. Dann gilt:
$|U| \mid |A|$ und $|A/U| = \frac{|A|}{|U|}$
(b) *Kleiner Satz von Fermat:*
Sei $p \in \mathbb{N}$ eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$.
Dann gilt:
$a^{p-1} \equiv 1 (modulo p)$
d.h. $p \mid a^(p-1)-1$

Beweis:

(a) (1) A/U bildet eine Partition von A (die Restklassen modulo U sind die Fasern der kanonischen Abb. π).
(2) Für alle $a \in A$ ist die Abb.
$U \to a+U$, $u \to a+u$ eine Bijektion.
Aus (1) + (2) folgt die Behauptung.
(b) Für $x \in \mathbb{Z}$ sei $\bar{x} := x + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$.
$\mathbb{Z}/p\mathbb{Z}$ ist Körper. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$
$\Rightarrow (\underbrace{\mathbb{Z}/p\mathbb{Z}^*}_{\mathbb{Z}/p\mathbb{Z}\setminus\{0\}}, \cdot)$ ist Gruppe.
$p \nmid a \Rightarrow \bar{a} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$
$\Rightarrow$ Die Folge $\bar{a}, \bar{a}^2 = \bar{a} \cdot \bar{a}$, ... wiederholt sich ($\mathbb{F}_p^*$ ist endlich).
$\Rightarrow$ es ex. $1 \leq i < j \in \mathbb{N}$ mit $\bar{a}^i = \bar{a}^j \Rightarrow \bar{a}^{i-j} = \bar{1}$
Sei $k \in \mathbb{N}$ minimal mit $\bar{a}^k = \bar{1}$.
$\Rightarrow \bar{a}, \bar{a}^2, ..., \bar{a}^{k-1}, \bar{a}^k = 1$ sind paarweise verschieden.
$U := \{\bar{a}, \bar{a}^2, ..., \bar{a}^{k-1}\}$ ist Untergruppe von $\mathbb{F}_p^*$
$\bar{a}^i \cdot \bar{a}^j = \bar{a}^{i+j} = \bar{a}^r$, falls $i+j = qh+r$ mit $0 \leq r < k$
$\bar{a}^{-1} = \bar{a}^{k-1}$ (Inverses)
$\bar{a}^{-2} = \bar{a}^{k-2}$ etc
Aus (a) folgt: $k = |U| \nmid |(\mathbb{F}_p^*, \cdot)| = p-1$
Sei $p-1 = qk \Rightarrow \bar{a}^{p-1} = \bar{a}^{qk} = (\bar{a}^k)^q = \bar{1}^q = \bar{1}$

1.3 Beispiel

Sei p = 5.
$a \in \mathbb{Z}, 5 \nmid a \Rightarrow a^4 - 1$ ist durch 5 teilbar.
$a = 2, 2^4 - 1 = 16 - 1 = 15$
$a = 8, 8^4 - 1 = 4096 - 1$
$8^4 \equiv (8^2)^2 \equiv (-1)^2 \equiv 1 (mod 5)$

1.4 Bemerkung

Die Konstruktion aus (1.1) (Restklassen) macht auch Sinn für nicht-abelsche Gruppen.
Sei $(G, \cdot)$ Gruppe, $H \leq G, g \in G$

$gH := \{g \cdot k | k \in H\}$ Restklasse
$G/H := \{gH | g \in G\}$ Menge der Restklassen
I.A. ist G/H keine Gruppe (mit der zu (1.1) analogen Konstruktion.

Beispiel:

$G = S_3, H =< (1\ 2) >= \{1, (1\ 2)\}$
Restklassen:
$H = 1H = \{1, (1\ 2)\}$
$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$
$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H$
$((1\ 3)(1\ 2\ 3) = (1\ 2))$
Wie müssten wir gemäß (1.1) $1H \cdot (1\ 3)H$ definieren?
$\underbrace{(1H)}_{=(1\ 2)H} \cdot (1\ 3)H = (1)(1\ 3)H = (1\ 3)H$
$(12)H \cdot (1\ 3)H = (1\ 2)(1\ 3)H = \underbrace{(1\ 3\ 2)}_{\neq(1\ 3)}H$
$\Rightarrow$ nicht repräsentanten-unabhängig! $1, (1\ 2)$ sind die Repräsentanten der Restklasse. Die Anwendung von (1.1) ergibt keine *wohldefinierte* Verknüpfung.
Aber: $H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$
Restklasse: $H = 1H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$
$(1\ 2)H = \{(1\ 2), (2\ 3), (1\ 3)\}$
Hier gilt: $a \cdot b \in H\ \forall a, b \in H$ und $a \cdot b \in H\ \forall a, b \in (1\ 2)H$ und $a \cdot b \in (1\ 2)H$, falls a und b in verschiedenen Restklassen liegen.
$\Rightarrow G/H$ ist Gruppe (mit der Verknüpfung aus (1.1))

1.5 Definition

Sei R ein kommutativer Ring, $I \leq (R, +)$ heißt **Ideal**, geschrieben $I \trianglelefteq R$, falls gilt:
$r \cdot a \in I\ \forall r \in R, a \in I$

1.6 Beispiel

Sei R ein kom. Ring
$a \in R \Rightarrow a \cdot R := \{ar | r \in R\} \trianglelefteq R$
(Bemerkung von mir: Das ist zufällig auch ein Hauptideal, da I von a erzeugt wird. Hauptideale sind die am einfachsten zu bildenden Ideale)

1.7 Definition und Bemerkung

(a) Sei K ein Körper, V K-VR, $U \leq V$. Dann ist
V/U ein K-VR mit der Addition aus (1.1) und der skalaren Multiplikation
$\cdot : V/U \times V/U \to V/U, a \to a \cdot (v+U) := (av) + U$
Die kanonische Abb. $\pi : V \to V/U, v \to v+U$ ist ein surjektiver Homomorphismus.
(b) folgt (?)

Beweis:

Skalare Multiplikation wohldefiniert:
Sei $a \in K, v, v' \in V$ mit $v+U = v'+U$
$\Rightarrow v-v' \in U \Rightarrow a(v-v') \in U \Rightarrow av-av' \in U$
$\Rightarrow av+U = av'+U$

1.8 Satz - PlatzhalterSatz fuer spaeter

XXX ———————— Hier einige Auslassungen

Randbemerkung

Jeder VR der Form V/U heißt *Faktorraum*.

1.9 Satz (Isomorphie-Satz)

K Körper, V K-VR, $U, W \leq V$
$(U+W)/U \cong W/(U \cap W)$

Beweis

Betrachte:
$\varphi : W \to (W+U)/U, w \to w+U$
φ ist K-linear.
φ ist surjektiv: $(w+u)+U = w+U = \varphi(w)$ für $w \in W, u \in U$
Kern $\varphi = W \cap U$: Für w $in W$ gilt:
$w \in$ Kern $\varphi \Leftrightarrow w+U = 0 \Leftrightarrow w \in U \cap W$
$\Leftarrow (1.10) (W+U)/U =$ Bild $\varphi \cong W/(\text{Kern}\varphi) = W/(W \cap U)$

1.10 Korrolar

Sei K Kp, V K-VR, $U, W \leq V$. Dann gilt:
$dim_K(W+U) + dim_K(W \cap U) = dim_K(W) + dim_K(U)$

Beweis

$dim_K(W+U) - dim_K(U) = dim_K((W+U)/U) \underbrace{=}_{(1.9)} dim_K(W/(W \cap U)) = dim_K(W) -$

$dim_K(W \cap U)$

2 Der euklidische Algorithmus

R kommutativer Ring, K Körper

2.1 Definition

(a) $a \in R$ heißt *Nullteiler*, falls $a \neq 0$ ist und ein $b \neq 0$ ex. mit $ab = 0$
(b) R heißt *Integritätsbereich (IB)*, falls $R \neq \{0\}$ ist und R keine Nullteiler hat.

2.2 Beispiele

(a) K ist IB.
(b) $\mathbb{Z}$ ist IB
(c) Sei $m \in \mathbb{N}, m \geq 2$. Dann gilt: $\mathbb{Z}/m\mathbb{Z}$ ist IB $\Leftrightarrow$ m Primzahl.
(d) $K[X]$ ist IB.

Beweis

(a), (b), (d) klar
(c) "$\Rightarrow$"
Sei m keine Primzahl $\Rightarrow m = a \cdot b$ mit $1 < a, b < m$
$\Rightarrow a + m\mathbb{Z} \neq 0 \neq b + m\mathbb{Z}$
aber $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = ab + m\mathbb{Z} = m + m\mathbb{Z} = 0$
"$\Leftarrow$"
m Primzahl $\Rightarrow \mathbb{Z}/m\mathbb{Z}$ ist Körper.

2.3 Definition

R heißt *euklidischer Ring*, falls R ein IB ist, und eine Abb. (*Normaabbildung*)
$\nu : R \setminus \{0\} \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$
ex., so daß gilt:
Zu $a, b \in r$ mit $b \neq 0$ ex. $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\nu(r) < \nu(b)$ (Division mit Rest)

2.4 Beispiele

(a) $R = \mathbb{Z}, \nu(a) = |a|$ für $a \neq 0$
(b) $R = K[X], \nu(f) = deg(f)$ für $f \neq 0$
(c) $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ $(i^2 = -1)$ $\nu(a + bi) = a^2 + b^2$, für $(a, b) \neq (0, 0)$
(d) $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ $\nu(a + b\sqrt{2}) = a^2 + 2b^2, (a, b) \neq (0, 0)$

Beweis

(a),(b) klar, (c), (d) Übung

2.5 Definition

Seien $a, b \in R$

(1) $a|b$ (a *teilt* b) :$\Leftrightarrow$ ex ex. $c \in R$ mit $a \cdot c = b (\Leftrightarrow b \in aR = \{ar | r \in R\})$

(2) $d \in R$ heißt größter gemeinsamer Teiler von a und b, geschrieben $d = ggT(a,b)$ (engl. *gcd*), falls gilt

(a) $d|a$ und $d|b$

(b) Ist $d' \in R$ mit $d'|a$ und $d'|b$, dann gilt $d'|d$

Für $a = b = 0$ definieren wir $ggT(a,b) = 0$.

Bemerkung

In *euklidischen* Ringen:

Zu $a, b \in R$ ex. $ggT(a,b)$

Außerdem: ex. $x, y \in R$ mit $ggT(a,b) = ax + by$.

2.6 Bemerkung

Seien $d, q, a, b, c \in R$ mit $c = a + qb$. Dann gilt:

$d = ggT(a,b) \Leftrightarrow d = ggT(b,c)$

Beweis

$a = c + (-q)b$

Deshalb genügt es "$\Rightarrow$" zu beweisen.

(a) $d|a$ und $d|b \Rightarrow d|b$ und $d|c = a + qb$

(b) Sei $d' \in R$ mit $d'|b$ und $d'|a = c - qb \underbrace{\Rightarrow}_{d = ggT(b,c)} d'|d \Rightarrow d$ ist $ggT(b,c)$

2.7 Satz - EEA: Erweiterter Euklidischer Algorithmus

Sei R ein euklidischer Ring mit Normabb. $\nu : R \setminus \{0\} \to \mathbb{N}_0$.

Seien $a, b \in R$.

Dann ex. $x, y \in R$, so daß $d = ax + by$ ein ggT von a und b ist.

Der folgende Algorithmus berechnet d, x, y.

Algorithmus: (EEA)

Eingabe: $a, b \in R$

Ausgabe: $d = ggT(a,b), x, y \in R$ mit $d = ax + by$

(Hier: ν = nu")

```
BEGIN

  r_0 := a
  r_1 := b
  x_0 := 1
  x_1 := 0
```

```
  y_0 := 0
  y_1 := 1

  i := 1

  WHILE r_i != 0 DO
    Definiere r_i+1 durch
      r_i-1 := q_i * r_i + r_i+1    (mit r_i+1 = 0 oder nu(r_i+i) < nu(r_i))
    x_i+1 := x_i-1 - q_i * x_i
    y_i+1 := y_i-1 - q_i * y_i
    i = i + 1
  ENDWHILE

  d := r_i-1
  x := x_i-1
  y := y_i-1

END.
```

Beweis

1. Fall: $b = 0$

$r_1 = 0$, while-Schleife wird nicht durchlaufen.

$i = 1, r_{i-1} = r_0 = a$

$a = ggT(a,0)$

$x = x_0 = 1, y = y_0 = 0$

$a = xa + yb$

2. Fall: $b \neq 0$

In jedem Durchlauf der while-Schleife wird $\nu(r_{i+1}) \in \mathbb{N}_0$ kleiner (oder $r_{i+1} = 0$)

$\Rightarrow$ die Schleife wird nur endlich oft durchlaufen.

Sei n der Wert von i beim letztmaligen Durchlaufen der while-Schleife (vor der Erhöhung von i)

$\Rightarrow r_{n+1} = 0, r_{n-1} = q_n \cdot r_n$ und r_n wird als d ausgegeben.

Für $1 \leq i \leq u$ gilt: $r_{i-1} = q_i r_i + r_{i+1}$

$\underbrace{\Rightarrow}_{2.6} ggT(a,b) = ggT(v_0,v_1) = ggT(v_1,v_2) = ... = ggT(r_{n-1},r_n) = ggT(r_n,r_{n+1}) = ggT(r_n,0) = r_n$

Zeige mit Induktion:

$r_i = ax_i + by_i$ für $0 \leq i \leq n$

$i = 0,1$ ok nach Def. von x_0, x_1, y_1, y_0

Sei $2 \leq i \leq n$.

$ax_i + by_i = a(x_{i-2} - q_{i-1}x_{i-1}) + b(y_{i-2} + q_{i-1}y_{i-1})$

$= \underbrace{ax_{i-2} + by_{i-2}}_{=r_{i-2}} - \underbrace{(ax_{i-1} + bx_{i-1})}_{=r_{i-1}} q_{i-1}$

$= r_{i-2} - r_{i-1}q_{i-1} = r_i$

2.8 Bemerkung

(a) Ohne die Berechnung von x, y heißt (2.7) der *euklidische Algorithmus (EA)*.
(b) Zur Berechnung des ggT brauchen wir nur 3 Speicherplätze.
Beispielprogramm: $R = \mathbb{Z}$
Eingabe: $a, b \in \mathbb{Z}$
Ausgabe: $d = ggT(a,b)$

```
BEGIN
  WHILE b != 0 DO
    r := a mod b
    a := b
    b := r
  END
  RETURN(|a|)
END.
```

2.9 Beispiel

$R = \mathbb{Z}, a = 1955, b = 68$
$r_0 = 1955, r_1 = 68, x_0 = 1, x_1 = 0, y_1 = 1, y_0 = 0$
$1955 = 26 \cdot 68 + 51 \qquad x_2 = x_0 - q_1 x_1 = 1 \qquad y_2 = y_0 - q_1 y_1 = -28$
$68 = 1 \cdot 51 + 17 \qquad x_3 = x_1 - q_2 x_2 = -1 \qquad y_3 = y_1 - q_2 y_2 = 1 - 1 \cdot (-28) = 29$
$51 = 3 \cdot 17 + 0$
$r_4 = 0 \Rightarrow ggT(1955, 68) = 17$ und $17 = 1955 \cdot (-1) + 68 \cdot 29$

2.10 Bemerkung

Sei R euklidischer Ring und $I \trianglelefteq R$
Dann ex. $b \in I$ mit $I = bR$
(Ein Ideal der Form bR heißt *Hauptideal*. R ist ein $Hauptidealring$).

Beweis

$I = \{0\} \Rightarrow b = 0$ tut's.
(Trick 1): Sei $I \neq \{0\} und 0 \neq b \in I$ derart, daß $\nu(b)$ minimal unter allen $\nu(a), 0 \neq a \in I$
$bR \subseteq I$, da $b \in I$ und $I \trianglelefteq R$.
(Trick 2): Sei $a \in I \Rightarrow a = qb + r$ mit $r = 0$ oder $\nu(r) < \nu(b)$.
$r = a - qb \in I$, da $I \trianglelefteq R$
$\Rightarrow r = 0$ nach Wahl von b

3 Endliche Körper

3.1 Bemerkung

Sei K Körper und $K_0 \leq K$ ein Teilkörper (in diesem FAll heißt K eine Körpererweiterung von K_0.

(a) K ist K_0-VR

(b) Ist K ein e.d. K_0-VR und $x \in K$, dann ex. $d \in \mathbb{N}$, so daß $1, x, x^2, ..., x^d$ l.a. über K_0 ist.

Insbesondere ex. $f \in K_0[X]$, normiert, mit $f(x) = 0$.

Beweis

(a) Skalare Multiplikation:

$K_0 \times K \to K, (a, v) \to av$ $\quad \leftarrow$ Mul. in K

(b) Sei $n = dim_{K_0} K \Rightarrow 1, x, x^2, ..., x^n$ ist l.a. über K_0

$\Rightarrow$ es ex. $a_0, ..., a_d \in K_0$ mit $d \in \mathbb{N}, a_d \neq 0$ und $\sum_{i=0}^{d} a_i x^i = 0$

$\Rightarrow$ Beh.

3.2 Satz

(a) Sei K_0 ein Körper, $f \in K_0[X]$ irreduzibel mit $deg(f) = n$.

Sei $I = fK_0[X]$. Nach (1.8)(b) ist $K := K_0[X]/I$ ein Körper.

$\iota : K_0 \to K, a \to a + I$ ist injektiver Ring-Hom.

$\iota(K_0) \subseteq K$ ist Teilkörper.

K ist ein n-dim. $\iota(K_0)$-VR mit Basis $1, x, x^2, ..., x^{n-1}$ für $x := X + I$

Beweis

(a) ι ist die Komposition zweier Ringhom. $K_0 \to K_0[X] \to K_0[X]/I$, also Ringhom.

$\iota(a) = 0$

$\Rightarrow a + I = 0$

$\Rightarrow a \in I$

$\Rightarrow a = 0$, da $I = fK_0[X]$ und $deg(f) \geq 1$.

$\Rightarrow$ Kern $(\iota) = \{0\} \Rightarrow \iota$ injektiv

Sei $g \in K_0[X]$.*Schreibeg* $= qf + r$ mit $r = 0$ oder $deg(r) < grad(f)$

$\Rightarrow g + I = r + I \in < 1, x, x^2, ..., x^{n-1} >$ (K_0-VR Erzeugnis)

Seien $a_0, ..., a_{n-1} \in K_0 mit \sum_{i=0}^{n-1} \iota(a_i) x^i = 0$

$\Rightarrow \sum_{i=0}^{n-1} a_i x^i \in I = fK_0[X]$

$\Rightarrow \sum_{i=0}^{n-1} a_i x^i = 0$ (Grad!)

$\Rightarrow \iota(a_i) = 0 \quad 0 \leq i \leq n-1$

$\Rightarrow (1, x, ..., x^{n-1})$ ist $\iota(K_0)$-Basis von K.

(b) Sei $K_0 \leq K$ ein erweiterter Körper, so daß K ein n-dimensionaler K_0-VR ist. Sei $x \in K$ und $0 \neq f \in K_0[X]$ normiert und von minimalem Grad mit $f(x) = 0$ (f existiert nach (3.1).

Dann ist f irreduzibel und $K_0[X]/fK_0[X] \cong K_0[X] \leq K$

Beweis

Die Existenz von f folt aus (3.1).

Wäre $f = g \cdot h$ mit $1 < deg(g), deg(h) < deg(f)$, dann ist $f(x) = 0 = g(x)h(x)$, also $g(x) = 0$ oder $h(x) = 0$

$\Rightarrow$ Widerspruch zur Minimalität von $deg(f)$.

(Bild des Einsetzungshom.) $K_0[X] = \iota_x(K_0[X]) = \{h(x) | h \in K_0[X]\}$

$\underbrace{\Rightarrow}_{(3.1)}$ Kern $\iota_x) = fK_0[X]$

$\Rightarrow K_0[X]/fK_0[X] \cong K_0[X]$

3.3 Definition und Bemerkung

Sei $(A, \cdot)$ eine endliche abelsche Gruppe (multiplikativ geschrieben).

(a) Für $a \in A$) existiert $n \in \mathbb{N}$ mit $a^n = 1$

(b) Sei $a \in A$ und $n \in \mathbb{N}$ minimal mit $a^n = 1$, n heißt die *Ordnung* von a, geschrieben: $|a| := n$

Es gilt: $|a| \big| |A|$. Ist $z \in \mathbb{Z}$ mit $a^z = 1$, dann ist $|a| \big| z$. ($a^0 := 1, a^{-n} := (a^{-1})^n, n \in \mathbb{N}$).

(c) Sei $a \in A$. $< a >:= \{a^z | z \in \mathbb{Z}\} \leq A$ heißt die von a erzeugte Untergruppe von A.

Es gilt: $| < a > | = |a|$.

(d) A heißt *zyklisch*, falls $a \in A$ existiert mit $A =< a >$.

(e) Sei $e = max\{|a| | a \in A\} \Rightarrow a^e = 1 \forall a \in A$ (Beh.)

A ist eine endlich abelsche Gruppe.

Beweis

(vgl. den Beweis von (1.2)(b):

$a, a^2, a^3, ...$ wiederholt sich, d.h. es ex. $a \leq i < j \in \mathbb{N}$ mit $a^i = a^j$.

$\Rightarrow a^{ji} = 1, d.h.(a)$

Sei $n = |a|$

$\Rightarrow \{a, a^2, ..., a^n = 1\} \subseteq A$ mit $|\{a, a^2, ..., a^n = 1\}| = n$

$\underbrace{\Rightarrow}_{(1.2)(a)}$ $|a| = | < a > | \big| |A|$

Schreibe $z = qn + r$ mit $0 \leq r \leq n$

$\Rightarrow a = a^z = a^r \cdot (a^n)^q = a^r$

$\Rightarrow r = 0$ ((b), (c) jetzt bewiesen)

Beweis zu (e):

Sei $a \in A$ mit $|a| = e$. Angenommen, es ex. $b \in A$ mit $b^e \neq 1$.

$\Rightarrow n := |b| \not| e$

$\Rightarrow$ es ex. $p \in \P$ (Primzahl in $\mathbb{N}$) und $k \in \mathbb{N}$ mit $p^k | n$ aber $p^k \not| e$.

Sei $n = p^k \cdot m, e = p^l \cdot d$ mit $p \not| m, p \not| d (\Rightarrow k > l)$

Setze $a' := a^{p^l}$ und $b' := b^m$.

$\Rightarrow |a'| = d, |b'| = p^k$ (selbst), $ggT(p^k, d) = 1$

$\Rightarrow$ es ex. $x, y \in \mathbb{Z}$ mit $1 = p^k x + dy$

Hier fehlte mir die Zeit, das Skript fortzuführen.