

## Nachtrag über euklidische Ringe

Sie erhalten hier Beweise zum Lemma über euklidische Ringe, die in der Vorlesung weggelassen wurden, weil die Aussagen in den am meisten interessierenden Spezialfällen  $R = \mathbb{Z}$  und  $R = K[X]$  ohnehin klar sind. Wer über allgemeine euklidische Ringe Bescheid wissen will, sollte die Beweise genau nachlesen.

**Lemma** Sei  $R$  ein euklidischer Ring. Dann existiert eine Abbildung  $gr : R \rightarrow \mathbb{N}$ , für die  $R$  euklidisch ist und zusätzlich gilt:

- (i) Für  $e \in R^\times$  und  $a \in R$  gilt  $gr(ea) = gr(a)$ .
- (ii) Ist  $a, b \in R$ ,  $a \neq 0$  und  $b$  ein Teiler von  $a$ , so ist  $gr(b) \leq gr(a)$ , bei echtem Teiler ist sogar  $gr(b) < gr(a)$ .

**Beweis:**

- (i) Wir gehen von dem euklidischen Ring  $(R, gr)$  aus und verwenden

$$gr^*(a) := \min\{gr(ea) \mid e \in R^\times\}.$$

Dieses Minimum existiert, da jede nichtleere Menge natürlicher Zahlen ein Minimum besitzt, und wegen  $R^\times ea = R^\times a$  ist offenbar  $gr^*(ea) = gr^*(a)$ .

Nun ist zu beweisen:  $R$  ist euklidisch bezüglich  $gr^*$ .

Im Folgenden sei stets  $a, b \neq 0$ .

Zu  $b$  gibt es ein  $e \in R^\times$  mit  $gr(eb) = gr^*(b)$ . Dividiert man mit Rest  $a$  durch  $eb$ , so wird  $a = qeb + r$  mit  $r = 0$  oder  $gr^*(r) \leq gr(r) < gr(eb) = gr^*(b)$ . Dieses  $r$  ist also auch bezüglich  $gr^*$  als Rest bei Division von  $a$  durch  $b$  verwendbar. (i) ist also für die Größenfunktion  $gr^*$  richtig, die wir nun wieder mit  $gr$  bezeichnen wollen.

- (ii) Wir zeigen (1.Schritt)  $b \mid a \Rightarrow gr(b) \leq gr(a)$ .

Annahme: Das ist falsch. Dann gibt es Gegenbeispiel, nämlich ein Paar  $(a, b)$  mit  $b \mid a$ ,  $a \neq 0$  und  $gr(b) > gr(a)$ . Unter den  $a$  mit  $\exists b$  mit  $b \mid a$  und  $gr(b) > gr(a)$  gibt es eins mit minimalem  $gr(a)$ . Ist also  $gr(a') < gr(a)$ , so folgt aus  $b \mid a'$  immer  $gr(b) \leq gr(a')$ .

Wir dividieren mit Rest:  $b = qa + r$  mit  $r = 0$  oder  $gr(r) < gr(a)$ .  $r = 0$  führt zu  $a \mid b$ . Wegen  $b \mid a$  gibt es nach 1.2, Satz über elementare Teilbarkeitseigenschaften (iii), eine Einheit  $e$  mit  $a = eb$ , also  $gr(a) = gr(b)$ , Widerspruch. Die andere Möglichkeit, nämlich  $gr(r) < gr(a)$ , führt ebenfalls zu einem Widerspruch. Aus  $b \mid a$  folgt  $b \mid b - qa = r$  und da  $r$  ein  $a'$  wie oben ist, erhält man den Widerspruch  $gr(b) \leq gr(r) < gr(a)$ . Die Annahme muss also verworfen werden, und die Aussage ist richtig.

Verbleibt (2. Schritt): Ist  $b$  ein echter Teiler von  $a$ , so ist  $gr(b) < gr(a)$ .

Denn bei Division mit Rest  $b = qa + r$  geht  $r = 0$  nicht, da wie im 1. Schritt  $a = eb$  mit  $e \in R^\times$  wäre, also  $b$  kein *echter* Teiler. Also ist  $gr(r) < gr(a)$  und  $b \mid r$ , nach dem 1. Schritt also  $gr(b) \leq gr(r) < gr(a)$  und somit  $gr(b) < gr(a)$ , was zu zeigen war. **q.e.d.**