

---

# Prüfungsprotokoll

zur mündlichen Nebenfachprüfung Mathematik im  
Diplomstudiengang Informatik an der RWTH-Aachen

25.03.2009 (WS 2008/09)

Florian Weingarten

---

## Prüfungsinhalt:

- Computeralgebra (V4, SS 2008, Prof. Dr. Eva Zerz)
- Kommutative Algebra (V4, WS 2008/09, Prof. Dr. Eva Zerz)
- Algebraische Zahlentheorie I (V2, WS 2008/09, Prof. Dr. Aloys Krieg)

**Prüfer:** Frau Prof. Dr. Eva Zerz (Lehrstuhl D für Mathematik)

**Prüfungsdauer:** etwas mehr als 45 Minuten

**Prüfungsnote:** 1.0

**Achtung:** Hierbei handelt es sich *nicht* um ein offizielles Prüfungsprotokoll der RWTH sondern um ein privates Gedächtnisprotokoll, dass ca. 2 Stunden nach der Prüfung angefertigt wurde. Ich habe mit Sicherheit einige Sachen vergessen. Ausserdem sind Frau Zerz' Fragen natürlich keine „Zitate“ sondern nur „irgendwie sowas in der Art hat sie gesagt“ :-)

Frau Zerz fragt mich, ob ich eine bevorzugte Reihenfolge habe. Ich wähle Computeralgebra als erstes. Die Abgrenzungen sind allerdings **sehr** schwammig, da ich lauter Querverweise auf die jeweils anderen Vorlesungen gegeben habe und Sie daraufhin lauter Fragen hinterher geschickt hat, die eigentlich nicht zu der momentanen Vorlesung gehörten.

## §1 Computeralgebra

**EZ:** Ok, fangen wir mal einfach an. Prim und irreduzibel. Was ist das?

**FW:** Ein Element  $p$  eines kommutativen Ringes, dass weder Nullteiler noch Einheit ist, nennt man prim, falls immer wenn es ein Produkt von zwei Elementen teilt, schon einer der Faktoren teilbar ist. Irreduzible Elemente sind die, die sich nicht als Produkt von zwei Nicht-Einheiten faktorisieren lassen. Primelemente sind irreduzibel, die Umkehrung ist aber i.A. falsch.

**EZ:** Warum sind die irreduzibel?

**FW:** Naja, wenn  $p = ab$ , dann folgt  $p|ab$ , ... Ääh.. Was wollte ich machen...

*Hier bin ich direkt schon sehr nervös geworden, weil der Beweis eigentlich völlig trivial ist.*

**EZ:** Sie wollten benutzen, dass  $p$  prim ist.

**FW:** Achja, klar. Genau. Also OBdA  $p|a$ , dann existiert also ein  $s$  mit  $ps = a$ , also  $p = ab = psb$ . So, da das  $p$  aber ja per Definition kein Nullteiler ist, gilt die Kürzungsregel und wir bekommen direkt  $1 = sb$ , also war  $b$  eine Einheit.

**EZ:** Genau. Was ist jetzt mit der anderen Richtung?

**FW:** Die ist nicht immer erfüllt. Wenn wir z.B. den quadratischen Zahlkörper  $\mathbb{Q}(\sqrt{-5})$  angucken, dann kann man die 6 in dessen Ganzheitsring auf zwei verschiedene (nicht-assoziierte) Arten in irreduzible zerlegen, nämlich  $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ . Also, Zerlegungen in irreduzible habe ich natürlich immernoch, aber die ist nichtmehr eindeutig, wie das sonst bei faktoriellen Ringen der Fall ist.

**EZ:** Und?

**FW:** Naja, 2 ist jetzt hier irreduzibel, aber nicht prim, denn es teilt ja die zweite Darstellung, ohne einen der Faktoren zu teilen. Das kann man über die Norm zeigen.

**EZ:** Wann gilt die andere Richtung denn doch?

**FW:** Bei faktoriellen Ringen. Das ist sogar äquivalent... Ääh.. Nein... Da fehlt noch was.

**EZ:** Ja, genau, was fehlt? Denken Sie mal an  $O_K$ .

**FW:** Noethersch glaube ich. Wenn der Ring noethersch ist, dann ist (prim  $\Leftrightarrow$  irreduzibel) äquivalent dazu, dass der Ring faktoriell ist.

**EZ:** Okay. Was ist ein Bezout Ring?

**FW:** Das ist so eine Art Verallgemeinerung von Hauptidealringen. Jedes endlich erzeugte Ideal ist ein Hauptideal (aber es kann eventuell welche geben, die überhaupt nicht endlich erzeugt werden können).

**EZ:** Nennen Sie mal ein Beispiel für einen Bezout Ring.

**FW:** Naja, jeder Hauptidealbereich ist Bezout ...

**EZ:** Ja, das ist ja langweilig.

**FW:** Ääh. Ja, Ok. Dann der Ring der holomorphen Funktionen auf  $\mathbb{C}$ . Da gibt es solche Sinus Funktionen, die kann man nicht endlich erzeugen.

**EZ:** Ja, genau. Okay. Wie kann man Bezout *Bereiche* denn charakterisieren?

**FW:** Hmmm... Sie meinen das mit den Silvesterringen?

**EZ:** Nein nein, das kommt später. Denken Sie mal an freie und torsionsfreie Moduln.

**FW:** Ähh. Die Untermoduln von freien sind dann torsionsfrei?

**EZ:** Das gilt aber ja immer

**FW:** Ähh. Klar. Hmmm...

**EZ:** Wann folgt denn aus torsionsfrei frei?

**FW:** Naja, das haben wir ja in LA2 schon gesehen, dass gilt für e.e. Moduln über Hauptidealbereichen nach dem Struktursatz.

**EZ:** Ja, na gut. Worauf ich hinaus wollte ist, dass  $R$  genau dann Bezout ist, wenn jeder endlich erzeugte torsionsfreie Modul frei ist.

**FW:** Ah, okay.

**EZ:** Okay, was ist mit  $K[x_1, \dots, x_n]$ . Ist der Bezout?

**FW:** Ja. Und Noethersch.

*Das ist natürlich falsch. Der ist nicht Bezout (sonst wär es ja bereits ein Hauptidealbereich). Bin mir nicht sicher, ob ich das falsch in Erinnerung habe oder ob ich das tatsächlich so gesagt habe.*

**EZ:** Was heisst noethersch überhaupt?

**FW:** Jedes Ideal ist endlich erzeugt. Bzw. jeder Untermodul ist endlich erzeugt, wenn wir von noetherschen Moduln ausgehen. Äquivalent dazu, erfüllt der Modul (bzw. Ring) diese Aufsteigende-Ketten-Bedingung.

**EZ:** Nennen Sie mal ein Beispiel.

**FW:** Der Ganzheitsring von algebraischen Zahlkörpern ist immer noethersch.

**EZ:** Öh. Ja, moment, nennen Sie mal ein etwas weniger abgefahrenes Beispiel.

**FW:** Standardbeispiel ist natürlich  $\mathbb{Z}$ . Oder  $\mathbb{Z}[X]$ , etc. Man kann dann übrigens sagen, dass ein Ring noethersch ist, genau dann, wenn er als Modul über sich selbst noethersch ist. Und andersherum kann man sich überlegen, dass Moduln über noetherschen Ringen wieder noethersch sind.

**EZ:** Sind sie sicher? Dann wäre ja jeder  $\mathbb{Z}$ -Modul noethersch.

**FW:** Ääääh...

**EZ:** Der Modul muss noch etwas erfüllen.

**FW:** Äh. Er muss endlich erzeugt sein.

**EZ:** Genau. Also:  $K[x_1, \dots, x_n]$ . Warum ist der noethersch?

**FW:** Das folgt mit dem Satz von Gauss.. Ääh..

**EZ:** Nee, das war etwas anderes.

**FW:** Ja, klar, Hilbert wars. Hilbertscher Basissatz.

**EZ:** Genau. Okay. Was ist eine Gröbnerbasis?

**FW:** Wenn wir ein Ideal  $I$  in  $K[x_1, \dots, x_n]$  haben, dann nennt man eine endliche, nicht-leere Teilmenge von  $I$  eine Gröbnerbasis, wenn  $\text{grad}(F) + \mathbb{N}^n = \text{grad}(I)$  gilt. Wobei  $\subseteq$  natürlich immer gilt. Also, man muss da natürlich erstmal eine Ordnung fixieren.

**EZ:** Warum fordert man nicht, dass  $F$  das  $I$  erzeugt, wie der Name es andeutet?

**FW:** Das folgt automatisch mit Division mit Rest nach  $F$ , denn ich kann jedes Element aus  $I$  schreiben als zulässige Kombination von  $F$ .

**EZ:** Also?

**FW:** Also ist  $\langle F \rangle = I$

**EZ:** Ok, schön. Wie löst man denn jetzt damit algebraische Gleichungssysteme?

**FW:** Naja, wir können jedes algebraische Gleichungssystem als endlich erzeugtes Ideal interpretieren. Dann bestimmt man eine Gröbnerbasis mit dem Buchberger-Algorithmus. Und dann.... Hm.. Naja, wenn das Ideal nulldimensional ist, dann kann man die Lösungen alle ausrechnen.

**EZ:** Nulldimensional?

**FW:** Naja, diese Gradmenge da,  $\text{grad}(F) + \mathbb{N}^n$ , deren Komplement muss endlich sein, dann nennt man das  $I$  nulldimensional.

**EZ:** Und was hat das mit den Lösungen zutun?

**FW:** Ja, wir haben dann gesehen, dass das äquivalent dazu ist, dass für jedes  $x_i$  mindestens ein  $f$  in  $I$  vorkommt, dass nur von dieser Variable abhängt. Dann wählt man sich eine lexikografische Ordnung, die dieses  $x_i$  minimal hat und bestimmt eine Gröbnerbasis. Dann bekommt man irgendwie (?) diese „Dreiecksform“ und kann Rückwärts einsetzen.

**EZ:** Genau. Sie haben gerade gesagt, dass die Lösungsmenge von Nulldimensionalen Idealen immer endlich ist.

Wie siehts mit der Umkehrung aus?

**FW:** Da muss man etwas aufpassen. Die Umkehrung ist im Allgemeinen nämlich falsch, gilt aber nach dem Hilbertschen Nullstellensatz über algebraisch abgeschlossenen Körpern.

**EZ:** Was sagt der Nullstellensatz denn?

**FW:** Naja, da hatten wir eigentlich drei Versionen. Die erste sagt nur  $V(I) = \emptyset \Leftrightarrow 1 \in I$ . Die zweite sagt, dass wenn  $L$  als  $K$ -Algebra endlich erzeugt ist,  $L/K$  bereits endlichen Grad hat. Und die dritte ist die interessanteste, die besagt, ... Äh.. also.. Es gibt ja ausser dem  $V(\cdot)$  auch noch so ein  $I(\cdot)$ , was der Varietät wieder ihr Ideal zuordnet. Dann gilt immer  $V(I(V)) = V$ . Der Hilbertsche Nullstellensatz sagt jetzt etwas über die andere Richtung, nämlich  $I(V(I))$ , da kann man nämlich eventuell mehr bekommen, das ist nämlich genau das Radikalideal von  $I$ .

*Habe jetzt noch irgendwas gestammelt von Koordinatenring und Nulldimensional... War sehr chaotisch. Hat ihr dann aber gereicht.*

**EZ:** Was heisst denn algebraisch abgeschlossen eigentlich?

**FW:** Naja, die „einfachste“ Definition ist, dass die irreduziblen Polynome genau die von Grad 1 sind, d.h. jedes Polynom höheren Grades zerfällt in Linearfaktoren. Alternativ kann man auch einfach sagen, dass der Körper keine echten endlichen Erweiterungen hat.

**EZ:** Was wissen sie über endliche Erweiterungen?

**FW:** Die sind immer algebraisch, denn wenn  $L$  als  $K$ -Vektorraum Dimension  $n$  hat, dann sind die  $n + 1$  Elemente  $1, \alpha^1, \dots, \alpha^n$  linear abhängig, und dann bekommt man damit ein Polynom geschenkt.

**EZ:** Okay, was ist die Idee bei quadratfreier Faktorisierung?

**FW:** Hmm. Das ging über den ggT mit der Ableitung, und dann.. ääääh...

**EZ:** Was ist mit dem ggT der Ableitung? Was hat das mit Quadratfreiheit zutun?

**FW:** Hm. Naja, wenn wir in Charakteristik 0 sind, dann ist ein Polynom genau dann quadratfrei, wenn der ggT mit seiner Ableitung gleich 1 ist. Also, die eine Richtung ist natürlich klar, wenn ich  $f = g^2h$  schreiben kann, dann ist  $f' = 2gg'h + g^2h'$ , also beide durch  $g$  teilbar. Die andere Richtung geht irgendwie über die Primfaktorzerlegung.

**EZ:** Ja genau. Braucht man das Charakteristik 0 ist wirklich?

**FW:** Hm. Also dann klappt das auf jedenfall immer. Z.B. bei  $x^2 \in \mathbb{F}_2[x]$ , da gehts schief, denn das ist nicht quadratfrei.

**EZ:** Ja, Okay. Das gilt aber auch in endlichen Körpern.

**FW:** Hm. Ich hab doch gerade ein Gegenbeispiel gebracht.

**EZ:** Hm. Moment.. Jetzt bin ich auch gerade verwirrt. Machen wir mal weiter.

*Mein Gegenbeispiel war keins, weil  $x^2$  zwar nicht quadratfrei ist, aber auch nicht ggT=1 mit seiner Ableitung hat (Ableitung ist das Nullpolynom). Siehe weiter unten, da wird das noch geklärt, als Frau Zerz merkt, dass ich da was falsches erzählt habe :-)*

**EZ:** Wie rechnet man denn so einen ggT überhaupt aus?

**FW:** Naja, in  $K[x]$  ist das einfach, der ist ja euklidisch. Der euklidische Algorithmus ist in seiner naiven Form aber ziemlich hässlich, weil da sehr böse Koeffizienten auftreten können. Wir hatten dann noch den modularen ggT Algorithmus. Die Idee war, dass ich viele Primzahlen  $p$  wähle und dann versuche den ggT in  $\mathbb{Z}_p$  zu bestimmen und dann damit auf den eigentlichen ggT schliessen kann.

**EZ:** Ja, so ungefähr. Was für  $p$  sind das?

**FW:** Das kann schiefgehen, wenn das  $p$  die Leitkoeffizienten teilt. Wenn das nicht passiert, dann heißt das  $p$  „gut“ und wir haben gezeigt, dass es nur endlich viele Primzahlen gibt, die für zwei Polynome nicht gut sind, also terminiert der Algorithmus.

**EZ:** Genau. Gut, brauchen wir noch was zur Gruppentheorie. Satz von Cauchy.

**FW:** Ja, also wir haben eine endliche Gruppe. Dann gibt es zu jedem Primteiler der Gruppenordnung ein Element der Ordnung. Und damit dann auch eine Untergruppe. Das ist quasi ein Spezialfall vom ersten Sylowsatz, der sagt, dass das nicht nur für die Primteiler sondern auch für die Primpotenzteiler klappt, dann gibt es immer Untergruppen der Ordnung  $p^k$ . Wenn man jetzt weiss, dass Gruppen mit Primzahlordnung zyklisch sind, dann bekommt man Cauchy geschenkt.

## §2 Algebraische Zahlentheorie I

**EZ:** Was ist eine quadratische Körpererweiterung?

**FW:** Naja, allgemein ist eine algebraische Körpererweiterung eine endliche Erweiterung von  $\mathbb{Q}$ , die ein Unterkörper von  $\mathbb{C}$  ist. Quadratisch nennt man die jetzt, wenn sie Grad 2 hat.

**EZ:** Okay, was können Sie denn über die Minimalpolynome sagen?

**FW:** Die teilen immer den Grad der Erweiterung, nach Gradsatz. Und im quadratischen Fall kann man die sogar ganz leicht angeben, da ist das nämlich  $X^2 - Sp(\alpha) \cdot X + N(\alpha)$ , also, ausser wenn  $\alpha \in \mathbb{Q}$ , dann ist das Minimalpolynom natürlich von Grad 1.

*Es muss natürlich heissen, dass der Grad des Minimalpolynoms den Grad der Erweiterung teilt. Bin mir aber ziemlich sicher, dass ich das in der Prüfung falsch gesagt habe.*

**EZ:** Und was bedeutet Spur und Norm jetzt?

**FW:** Hier ist das sehr schön einfach: Die Spur ist einfach  $\alpha + \bar{\alpha}$  und die Norm ist  $\alpha \cdot \bar{\alpha}$ , wobei  $\bar{\cdot}$  hier sowas wie die komplexe Konjugation ist, d.h.  $a + b\sqrt{m} \mapsto a - b\sqrt{m}$ .

**EZ:** Okay, moment. Sie haben ja jetzt hier noch etwas benutzt, was garnicht so klar ist eigentlich.

**FW:** Ääh.

**EZ:** Naja, was ist denn das für ein  $\sqrt{m}$ .

**FW:** Achso, ja, klar, man kann sich relativ einfach überlegen, dass *alle* quadratischen Zahlkörper von der Form  $\mathbb{Q}(\sqrt{m})$  sind wobei  $m \in \mathbb{Z} \setminus \{0, 1\}$  und quadratfrei. Also, das quadratfrei braucht es nicht unbedingt zu sein, es darf nur kein Quadrat sein, dann kann ich aber immer eine quadratfreie  $m$  finden, was die gleiche Erweiterung erzeugt.

**EZ:** Okay, und was ist jetzt der Ganzheitsring?

**FW:** Das ist quasi eine Verallgemeinerung von  $\mathbb{Z}$  in  $\mathbb{Q}$ . Das sind die sogenannten „ganzen Zahlen“ in  $K$ . Das ist per Definition genau die Menge der Zahlen, deren Minimalpolynom in  $\mathbb{Z}[X]$  ist. Hier also genau die, deren Norm und Spur in  $\mathbb{Z}$  sind, denn das sind ja die einzigen Koeffizienten. Im Allgemeinen ist das etwas komplizierter. Da definiert man sich erstmal nur, dass  $\alpha$  Nullstelle irgendeines normierten Polynoms in  $\mathbb{Z}$  sein muss.

**EZ:** Warum ist das äquivalent?

**FW:** Naja, die eine Richtung ist klar.

**EZ:** Stimmt.

**FW:** Für die andere Richtung:  $\mu_\alpha \in \mathbb{Q}[X]$ , etwa  $\mu_\alpha = \sum a_i x^i$ , dann gibt es aber einen Erweiterungskörper  $L$  in dem das Polynom zerfällt (das hatten wir ja auch in Computeralgebra gesehen), d.h. es gibt  $\alpha_i \in L$  (für irgendein  $L$ ), so dass  $\mu_\alpha = \prod (x - \alpha_i)$ . Wenn  $g \in \mathbb{Z}[X]$  jetzt irgendein Polynom ist, was  $\alpha$  als Nullstelle hat, dann ist es natürlich durch das Minimalpolynom teilbar, d.h. die  $\alpha_i$  sind auch alle ganz (in  $L$ ). Dann kann man sich leicht überlegen, dass die einzigen rationalen ganzen Zahlen die ganzen Zahlen in  $\mathbb{Q}$  sind, d.h.  $O_L \cap \mathbb{Q} = \mathbb{Z}$ . So, wenn ich das Polynom da oben jetzt ausmultipliziere, dann sieht man, dass die  $a_i$  alle von den  $\alpha_i$  abhängen, also sind die auch alle in  $\mathbb{Z}$ . Puh. :-)

**EZ:** Jetzt haben Sie aber ja eine Eigenschaft von  $O_K$  benutzt, die garnicht so offensichtlich ist.

**FW:** Hmm.. Naja, es ist halt ein Ring

**EZ:** Ja, warum ist das nicht klar? Das ist wie bei Computeralgebra mit der Menge der algebraischen Zahlen.

**FW:** Achso, klar. Naja, das ist eine relativ starke Aussage, denn wenn ich zwei ganze Elemente habe, muss ich ja garantieren, dass es ein Polynom gibt, das deren Summe als Nullstelle hat, das ist aber garnicht so klar, warum es sowas geben sollte, weil es keine direkte Möglichkeit gibt, das zu konstruieren. Hm. Naja, wir hatten sowas bei Computeralgebra in der Übung, aber das war sehr hässlich.

**EZ:** Hehe, ja. Wie haben wir das denn da gezeigt?

**FW:** Hm. Das ging irgendwie über den Gradsatz glaube ich. Dann wird das hier wohl auch irgendwie analog gehen.

**EZ:** Naja, nicht ganz. Was hat der Ganzheitsring denn sonst noch so für Eigenschaften?

**FW:** Hm. Naja, es ist immer ein Bereich. Dann kann man sich natürlich fragen, was der Quotientenkörper ist. Das ist genau das  $K$ , d.h. ich kann jedes Element aus  $K$  darstellen als Bruch von zwei Elementen von  $O_K$ . Man kann sich dann sogar überlegen, dass ich ohne Einschränkung die Nenner aus  $\mathbb{N}$  wählen kann.

**EZ:** Ja, genau. Gibt es sonst noch Zusammenhänge zu  $\mathbb{Z}$  und  $\mathbb{Q}$ ?

**FW:** Hmmm...

**EZ:** Welche Dimension hat  $O_K$  denn?

**FW:** Hmmm. Die Krulldimension kann schonmal nicht 0 sein, weil das Nullideal ja nicht maximal ist. Aber jedes andere Primideal ist maximal. Also ist die Dimension 1.

**EZ:** Genau wie  $\mathbb{Z}$  also. Sie hatten eben  $6 = 2 \cdot 3 = \dots$ . Was kann man daran sehr schön sehen?

**FW:** Dass  $O_K$  im Allgemeinen nicht faktoriell ist.

**EZ:** Genau. Was noch?

**FW:** Hmmm.. Naja, dass 2 nicht prim ist in  $O_{\mathbb{Q}(\sqrt{-5})}$ .

**EZ:** Genau. Was kann man denn allgemein über die Primzahlen aus  $\mathbb{N}$  sagen in  $O_K$ ?

**FW:** Im allgemeinen kann da ziemlich viel passieren. Im quadratischen Fall ist das aber noch relativ einfach. Da gibt es genau drei Fälle. Der „schöne Fall“, d.h.  $p$  ist hier auch selbst wieder prim, dann nennt man  $p$  träge. Dann gibt es noch den Fall verzweigt und zerlegt. Zerlegt heisst, dass ich  $\langle p \rangle$  schreiben kann als Produkt von zwei Primidealen

und verzweigt heisst, dass ich es... Naja.. auch als Produkt von zweien, aber zweimal das gleiche. Den Exponent nennt man dann übrigens Verzweigungsindex.

**EZ:** Genau. Okay, dann ...

**FW:** ... äh, was ich noch sagen wollte, man kann die verzweigten sogar sehr schön klassifizieren, das sind nämlich genau die, die die Körperdiskriminante teilen.

**EZ:** Was ist das denn?

**FW:** Naja, im Allgemeinen definiert man die Diskriminante einer  $\mathbb{Q}$ -Basis von  $K$ , und die Diskriminante des Körpers ist dann die Diskriminante einer Ganzheitsbasis.

**EZ:** Was ist das?

**FW:** Eine Gitterbasis von  $O_K$ , d.h. eine  $\mathbb{Z}$ -Basis. Und dann ist die Diskriminante sogar eine Invariante des Körpers.

**EZ:** Genau. So, was können Sie denn über die Einheiten im Ganzheitsring sagen?

**FW:** Im quadratischen Fall?

**EZ:** Ja

**FW:** Da unterscheidet man zwei Fälle. Also, erstmal: Man nennt so ein  $\mathbb{Q}(\sqrt{m})$  imaginär-quadratisch, wenn das  $m$  negativ ist, sonst reell-quadratisch. Im imaginärquadratischen Fall ist die Einheitengruppe gleich der Gruppe der Einheitswurzeln. Da gibt es dann drei Fälle oder so, wo die Gruppe Ordnung 2, 4 oder 6 hat. Beim reell-quadratischen Fall ist die Einheitengruppe unendlich. Das kann man z.B. in  $\mathbb{Q}(\sqrt{2})$  sehen, hier ist  $1 + \sqrt{2}$  eine Einheit. Das sieht man daran, dass Einheiten genau die Elemente sind, deren Norm  $\pm 1$  ist. Das ist hier so. Und jetzt ist jede Potenz davon natürlich wieder eine Einheit. Da die Potenzen aber immer größer werden, gibt es unendlich viele Einheiten.

**EZ:** Gut.

### §3 Kommutative Algebra

**EZ:** Welche Ränge für Matrizen hatten wir?

**FW:** Wenn wir über einem Bereich sind, nehmen wir natürlich den Rang im Quotientenkörper, im Sinne von LA, also Dimension des Spaltenraums. Dann hatten wir noch den inneren Rang, das ist definiert als  $\rho(A) := \min\{r \mid A_1 \cdot_r A_2 = A\}$ , wobei das  $r$  da die Spaltenzahl von dem  $A_1$  ist. Dieser Rang hat jetzt viele ähnliche Eigenschaften, z.B. ist er immer kleinergleich der Zeilen- und Spaltenanzahl, und wenn man ein Produkt hat, dann ...

**EZ:** Jaja, genau. Was ist jetzt ein Sylvesterring?

**FW:** Das ist ein Bereich, in dem ... Ach nein, moment, die Definition ist, dass immer wenn  $A \cdot_r B = 0$  ist, bereits  $\rho(A) + \rho(B) \leq r$  sein muss. Und das ist dann äquivalent dazu, dass der Ring ein Bereich ist, und der innere Rang mit dem klassischen Rang übereinstimmt.

**EZ:** Und was machen wir wenn wir nicht über einem Bereich sind?

**FW:** Hm, naja, dann können wir den reduzierten Rang angucken.

**EZ:** Was ist das?

**FW:** Also, erstmal:  $\text{rang}(A) = \max\{k \mid J_k(A) \neq 0\}$ , wobei das  $J_k$  hier das Ideal im Ring ist, dass von allen  $k \times k$ -Unterdeterminanten der Matrix  $A$  erzeugt wird. Der reduzierte Rang ist jetzt  $\text{redrang}(A) = \max\{k \mid \text{ann}(J_k(A)) = 0\}$ . Der reduzierte Rang ist jetzt immer kleinergleich dem Rang. Achso, beim inneren Rang ist übrigens der innere Rang i.A. größer. Wenn Rang und reduzierter Rang gleich sind, dann nennt man die Matrix (bzw. die Abbildung) rang-stabil.

**EZ:** Ja, genau. Was soll das jetzt? Wozu der reduzierte Rang? Sagen Sie mal was dazu?

**FW:** Hm. Sie meinen den Annihilator?

**EZ:** Nein nein, dass Sie wissen was DAS ist, glaube ich Ihnen auch so.

**FW:** Hmmmm. Ääh.. Ja.. Wozu.. Ich denke mal, die Motivation war, dass man analoge Aussagen zu LA wollte.

**EZ:** Welche?

**EZ:** Naja, z.B. der Satz von McCoy. Wenn ich eine lineare Abbildung zwischen zwei endlich erzeugten freien Moduln habe, etwa  $f : R^n \rightarrow R^m$ , dann sagt der Satz, dass die genau dann injektiv ist, wenn der reduzierte Rang  $n$  ist. Für surjektiv gibts was ähnliches, dann ist nämlich der reduzierte Rang gleich dem  $m$ . Die andere Richtung gilt hier allerdings nicht.

**EZ:** Genau, sehr schön. Was ist die Euler Charakteristik?

**FW:** Äh. Ja, da muss ich jetzt etwas ausholen. Also, wir können ja jeden Modul als Bild eines freien Moduls darstellen. D.h. es gibt immer so ein  $\pi : R^{(G)} \rightarrow M$  ( $(\cdot)$  heisst endlicher Träger), dann bekommt man ja so eine kurze exakte Sequenz geschenkt  $0 \rightarrow \ker \pi \rightarrow R^{(G)} \rightarrow M \rightarrow 0$ . So, jetzt ist der Kern aber wieder Bild eines freien, dann mache ich das nochmal, und immer so weiter. Wenn die auch noch alle endlich erzeugt sind, dann nennt

man das eine endlich freie Auflösung. Wenn das irgendwann terminiert, dann ist das eine endlich freie Auflösung endlicher Länge. So, d.h. die sieht irgendwie so aus:  $0 \rightarrow R^{r_0} \rightarrow \dots \rightarrow R^{r_n} \rightarrow M$ . Die alternierende Summe der  $r_i$  nennt man jetzt die Euler Charakteristik des Moduls. Da muss man eigentlich etwas vorsichtig sein, denn es könnte ja noch eine andere Auflösung geben, dann wären das andere  $r_i$ , aber das ist egal, denn das ist eine Invariante des Moduls. So, das ist jetzt hier so eine Teleskopsumme und da kommt dann  $E(M) = r_n + \text{rang}(f_n)$  raus.

**EZ:** Ja, sehr gut. Eine Kleinigkeit haben Sie noch vergessen.

**FW:** Hm. Naja. Die Pfeile sind alle Rangstabil.

**EZ:** Warum das?

**FW:** Naja, der erste ist rangstabil nach McCoy, weil er ja injektiv ist. Dann kann man sukzessiv weiter machen, wir hatten nämlich wenn  $R^n \rightarrow R^m \rightarrow R^l$ , und der erste Pfeil ist rangstabil, dann der zweite auch, das heisst die sind hier alle rangstabil.

**EZ:** Genau. Wann ist  $E(M) = 0$ ?

**FW:** Also in der Übung haben wir gesehen, dass das für Bereiche genau dann der Fall ist, wenn der Modul ein Torsionsmodul ist. Dann hatten wir noch einen Satz, den wir aber nicht bewiesen haben, Vasconcelos. Der sagt, dass  $E(M) = 0$  genau dann gilt, wenn  $\text{ann}(M) \neq 0$ .

**EZ:** Wann gibt es denn so eine endlich freie Auflösung endlicher Länge überhaupt?

**FW:** Öööh..

**EZ:** Kennen Sie da irgendeinen Spezialfall, wo man sogar die Länge begrenzen kann?

**FW:** Achso, klar.  $K[x_1, \dots, x_n]$ . Jeder Modul über diesem Ring hat eine endlich freie Auflösung von Länge  $\leq n$ . Das besagt gerade der Syzygiensatz von Hilbert.

*Glaube hier fehlt noch, dass der Modul endlich erzeugt sein muss. Scheint Frau Zerz aber nicht gemerkt (oder nicht gestört) zu haben.*

**EZ:** Genau. Was ist die Menge aller nilpotenten Elemente? Was hat das für eine Struktur?

**FW:** Das ist ein Ideal, das ist nämlich gerade der Schnitt aller Primideale.

**EZ:** Und die Menge der Nullteiler?

**FW:** Das hat gar keine Struktur. Das ist nämlich die Vereinigung von Idealen.. Und zwar die Vereinigung aller zu 0 assoziierten Primideale.

**EZ:** Was heisst das?

**FW:**  $P$  heisst assoziiert zu  $I$ , wenn  $P = (I : s)$  für ein  $0 \neq s \in R$ . Alternativ kann man sagen, dass das genau die primen Annihilatoren von Ringelementen sind.

**EZ:** Okay, und das mit den Nullteilern? Das klappt immer?

**FW:** Hm. Ja?

**EZ:** Nein, das klappt nur im noetherschen Fall. Sonst gilt nur eine Inklusion der Gleichheit.

*Gemeint war glaube ich, dass jedes zu Null assoziierte Primideal aus Nullteilern besteht. In nicht noetherschen Ringen könnte es aber noch weitere geben.*

**EZ:** Gut. Dann gehen Sie jetzt bitte kurz raus.

*Gefühlte 5 Sekunden später.*

**EZ:** Kommen Sie bitte wieder rein. Schauen Sie mal: Das was sie eben erzählt haben, mit  $x^2 \in \mathbb{F}_2[x]$ , das ist gar kein Gegenbeispiel, denn (...). Nur damit wir das noch geklärt haben :-)

**FW:** Ah, okay. Soll ich wieder raus?

**EZ:** Nein nein, sie bekommen natürlich eine 1.0, das war super.

**FW:** :-)

## §4 Fazit

Die Prüfung war sehr angenehm. Frau Zerz hat zwar vorallem in Kommutative Algebra sehr unerwarteten Stoff abgefragt (freie Auflösungen, Euler Charakteristik, keine einzige Frage zu irgendwelchen Funktoren, kein Lemma von Zorn, keine Idealzerlegungen, etc.), war aber sehr entgegenkommend, hat immer Tipps gegeben und mich ausreden lassen. Ich hatte generell das Gefühl, dass sie zwar sehr viel Stoff abgefragt hat, ich aber viel zu viel geredet habe. Ich habe meistens einfach alles erzählt, was mir eingefallen ist, auch wenn es nicht direkt die Frage beantwortet bzw. weit darüber hinaus geht (und das scheint ihr gefallen zu haben). Dafür, dass ich viele Kleinigkeiten nicht 100% korrekt beantwortet habe, war sie sehr fair.

Da ich absolut sicher bin, dass Frau Zerz irgendwann dieses Protokoll irgendwo in den Tiefen des Internets finden wird, möchte ich auf diesem Wege sagen: Vielen Dank für die tollen Vorlesungen! Jede der drei Vorlesungen, die ich bei Ihnen gehört habe, hat mir besser gefallen als die meisten Vorlesungen aus meinem Hauptfach!