Einige Fragen

Körper und Galoistheorie
WS 2009/2010

Zusammenfassung

Dies sind ein paar Fragen, die man sich im Laufe der Veranstaltung „Körper und Galoistheorie“ fragen könnte und die vielleicht nützlich sind, um sich auf eine Prüfung vorzubereiten. Einige Fragen gehen über den Inhalt der Vorlesung hinaus und einige in der Vorlesung behandelte Sachverhalte werden nicht erwähnt. Natürlich wird weder eine Garantie für die Richtigkeit der z.T. vorhandenen Antworten gegeben, noch eine Gewähr für irgendetwas übernommen.

Frage 1 Was ist eine Gruppe? Was ist ein Beispiel einer nicht abelschen Gruppe? Wieviele Element muss diese mindestens haben? Was ist eine Untergruppe? Was ist ein Normalteiler?

Frage 2 Was ist eine Faktorgruppe? Was ist das innere Produkt zweier Untergruppen einer Gruppe? Was ist das (direkte) Produkt zweier Gruppen? Was ist das semidirekte Produkt zweier Gruppen? Was sind die beiden behaldelten Isomorphiesätze?

Frage 3 Was ist eine Gruppenoperation? Was ist eine G-Menge? Was ist die Standgruppe, was ist der Orbit eines Elements? Beispiele!

Frage 4 Was ist eine p-Gruppe? Was ist eine Sylowgruppe? Wie lauten die Sylowsätze? Was sind (bis auf Isomorphie) alle Gruppen bis einschließlich Ordnung 8?

Frage 5 Was ist eine (endliche) Subnormalreihe, was ist eine (endliche) Normalreihe, was ist eine (endliche) Kompositionsreihe? Was ist eine auflösbare Gruppe? Was ist ein Beispiel einer auflösbaren und was ist ein Beispiel einer nicht auflösbaren Gruppe?

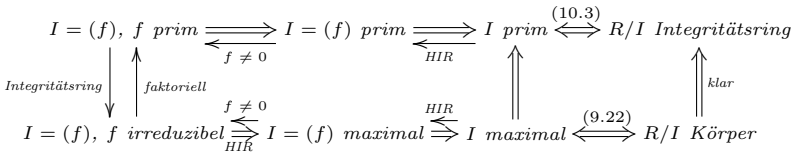
Antwort. *(Bitte auch die allgemeine Definition aus dem Skript lernen). Sei G eine Gruppe, eine endliche Subnormalreihe ist eine Folge*

$$\{e\} = G_n \rhd \ldots \rhd G_0 = G$$

von Gruppen. Ist jedes G_i auch Normalteiler in G, so heißt die Subnormalreihe eine Normalreihe. Sind alle Faktoren G_i/G_{i+1} einfach und nicht-trivial, so heißt die Subnormalreihe eine Kompositionsreihe. Die Gruppe G heißt auflösbar, wenn sie eine endliche Subnormalreihe mit (endlichen) abelschen Faktoren besitzt.
Es ist jede endliche abelsche Gruppe auflösbar. Die kleinste nicht auflösbare Gruppe ist A_5: Für $n \geq 3$ wird A_n von 3-Zykeln erzeugt. Für $n \geq 5$ sind alle 3-Zykel in A_n konjugiert (Achtung: $(1,2,3)$ und $(1,3,2)$ sind in A_4 nicht konjugiert). Daher ist A_n für $n \geq 5$ einfach, denn jeder nicht triviale Normalteiler von A_n erhält einen 3-Zykel und damit auch alle Konjugierten, also alle 3-Zykel. Wegen Einfachheit und nicht-Kommutativität ist A_5 nicht auflösbar.

Frage 6 Was ist ein Ring? Was ist ein Hauptidealring? Was ist ein faktorieller Ring? Was ist ein euklidischer Ring? Was ist ein maximales Ideal? Was ist ein Primideal? Beispiele! Was ist der Chinesische Restsatz? Was ist ein ggT, was ist ein kgV? Wie kann man sie finden?

Antwort. *Sei R ein kommutativer Ring mit Eins (hier wird gefordert $1 \neq 0$) und I ein Ideal in R und $f \in R$ ein Element. Es gelten die folgenden Implikationen (wieso?):*



Es ist der Polynomring $K[X]$ für einen Körper K ein euklidischer Ring und damit ein Hauptidealring. Ein Polynom f ist also irreduzibel genau dann, wenn f nicht konstant ist und f nicht als Produkt zweier nicht konstanter Polynome geschrieben werden kann, da $K[X]^* = K^* = K \setminus \{0\}$.

Frage 7 Was ist der „Satz von Vieta“ (bzw. der „Satz von den rationalen Nullstellen“)? Was ist das Eisenstein'sche Irreduzibilitätskriterium? Was kann man noch über Irreduzibilität sagen? Was ist eine Lokalisierung? Was ist ein Quotientenkörper?

Antwort. *Nach dem Satz 11.15 von Gauss ist ein irreduzibles und nicht konstantes Polynom aus $\mathbb{Z}[X]$ auch in $\mathbb{Q}[X]$ irreduzibel. Es gibt noch das folgende Irreduzibilitätskriterium:*

Lemma 0.1 *Sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom und p eine Primzahl. Ist $\bar{f}$ in $\mathbb{F}_p[X]$ (Quotienten modulo p) irreduzibel, so ist auch f irreduzibel.*

Denn ist $f = gh$ in $\mathbb{Z}[X]$ reduzibel, so gilt auch $\bar{f} = \bar{g}\bar{h}$ und der Grad bleibt invariant under der Reduktionsabbildung. Daher lässt sich $\bar{f}$ als Produkt zweier nicht konstanter Polynome schreiben und ist damit reduzibel.

Frage 8 Was ist ein Körper? Was ist eine Körpererweiterung? Was ist eine algebraische Körpererweiterung? Was ist das Minimalpolynom eines Elements? Was ist eine endliche Körpererweiterung? Was ist eine transzendente Zahl? Was ist die Charakteristik eines Rings?

Frage 9 Was ist eine einfache Körpererweiterung? Was ist ein primitives Element einer Körpererweiterung? Was ist ein Zerfällungskörper eines Polynoms und wieso existiert einer? Was ist ein algebraischer Abschluss eines Körpers und wieso existiert einer? Wieso sind Zerfällungskörper und algebraischer Abschluss bis auf Isomorphie eindeutig?

Frage 10 Was ist eine normale Körpererweiterung und was ist ein Beispiel für eine nicht normale Körpererweiterung?

Antwort. *Es ist $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ eine nicht normale Körpererweiterung, denn das Polynom $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ hat eine Nullstelle in $\mathbb{Q}(\sqrt[3]{2})$ aber es zerfällt nicht in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.*

Frage 11 Was ist eine separable Körpererweiterung und was ist ein Beispiel für eine nicht separable Körpererweiterung? Was ist ein perfekter Körper?

Antwort. *Da Körper der Charakteristik Null und endliche Körper perfekt sind, muss das Beispiel eine Erweiterung eines unendlichen Körpers der Charakteristik $p > 0$ sein. Bezeichne $\mathbb{F}_2(t)$ den Quotientenkörper des Polynomrings $\mathbb{F}_2[t]$. Das Polynom $X^2 + t \in \mathbb{F}_2(t)[X]$ ist irreduzibel (wieso?) aber nicht separabel, denn ist w eine Nullstelle, so gilt $(X + w)^2 = X^2 + w^2$ und w ist eine doppelte Nullstelle.*

Frage 12 Was ist der Satz vom primitiven Element? Was ist der Separabilitätsgrad und was ist der Inseparabilitätsgrad?

Antwort. *Nach dem Satz 16.15. vom primitiven Element ist jede endliche Körpererweiterung über einem perfekten Körper K (also z.B. $\mathbb{Q}$ oder ein endlicher Körper) einfach, d.h. von der Form $K(\alpha)$.*

Frage 13 Was ist die Galois-Gruppe $Gal(L, K)$ einer Erweiterung $K \subseteq L$? Was ist für eine Untergruppe von $Gal(L, K)$ der zugehörige Fixkörper? Was ist die Galois-Korrespondenz (Π, Ω)? Was ist eine Galois-Erweiterung und was sind dazu äquivalente Bedingungen?

Frage 14 Was ist die Galois-Gruppe eines Polynoms? Was ist die Diskriminante eines Polynoms und wofür ist sie beispielsweise gut?

Frage 15 Was ist eine primitive n-te Einheitswurzel und was ist eine zyklotomische Erweiterung? Was ist das n-te Kreisteilungspolynom? Was kann man über dessen Irreduzibilität sagen?

Antwort. *Sei K ein Körper. Eine n-te Einheitswurzel ist ein Element $a \in K$ dessen multiplikative Ordnung n teilt, d.h. ein Element für das gilt $a^n = 1$. Es ist die Menge der n-ten Einheitswurzeln $\mu_n(K)$ eine zyklische Untergruppe von $(K^*, \cdot)$ dessen Ordnung n teilt. Eine n-te Einheitswurzel a heißt primitiv, falls a auch tatsächlich die Ordnung n hat. Es heißt $K \subseteq Zer(X^n - 1)$ eine zyklotomische Erweiterung und ist die Charakteristik von K gut (d.h. entweder Null oder p mit $p \not| n$) so ist $Zer(X^n - 1) = K(a)$ für jede primitive n-te Einheitswurzel a. Das Produkt über alle primitiven n-ten Einheitswurzel a von $(X - a)$ heißt das n-te Kreisteilungspolynom und ist $K = \mathbb{Q}$, so ist dies irreduzibel und normiert und daher das Minimalpolynom einer jeden n-ten Einheitswurzel a. Über einem endlichen Körper muss das n-te Kreisteilungspolynom nicht irreduzibel sein. Beispiel: $(X^2 + 1) = (X + 3)(X + 2)$ ist das vierte Kreisteilungspolynom in $\mathbb{F}_5$.*

Frage 16 Was ist eine zyklische Erweiterung? Was ist Hilberts Satz 90? Was ist die Norm und was ist die Spur einer Körpererweiterung?

Antwort. *Eine zyklische Erweiterung ist eine Galoiserweiterung mit zyklischer Galoisgruppe. Ist K ein Körper mit einer guten Charakteristik (d.h. entweder Null oder p mit $p \not| n$) und $a \in K$ eine n-te Einheitswurzel, so ist $K(a)$ eine zyklische Erweiterung von K. Es gilt sogar noch mehr: Hat K gute Charakteristik und enthält eine primitive n-te Einheitswurzel, so ist die Erweiterung $K \subseteq Zer(X^n - b)$ zyklisch für alle $b \in K$ und die Ordung der Galoisgruppe teilt n.*

Frage 17 Was ist ein auflösbares Polynom? Wann heißt ein Polynom auflösbar?

Frage 18 Was wurde zur „Konstruktion mit Zirkel und Lineal“ gesagt? Wann ist das reguläre n-Eck mit Zirkel und Lineal konstruierbar?

Antwort. *Eine Fermat'sche Primzahl ist eine Primzahl der Form $2^i + 1$. Der Satz von Gauss sagt, dass das reguläre n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn $n = 2^i p_1 \dots p_m$, wobei die p_i verschiedene Fermat'sche Primzahlen sind.*

Frage 19 Wieviele endliche Körper gibt es?

Antwort. *Ein endlicher Körper $\mathbb{F}$ hat eine endliche prime Charakteristik $p > 0$ (keine Nullteiler) und daher den Primkörper $\mathbb{F}_p$. Ein endlicher Körper $\mathbb{F}$ ist ein Vektorraum über seinem Primkörper und hat daher p^n Elemente. Die Frobenius-Abbildung $F : \mathbb{F} \to \mathbb{F}$ mit $a \mapsto a^p$ ist ein Ringhomomorphismus, da $F(1) = 1$, $F(a+b) = (a+b)^p = a^p + b^p = F(a) + F(b)$ und $F(ab) = F(a)F(b)$. Es gilt $F^n = F \circ \ldots \circ F = \mathrm{id}_{\mathbb{F}}$ und der Frobenius-Homomorphismus ist die Identität auf dem Primkörper $\mathbb{F}_p$. Das Polynom $f = X^{p^n} - X$ zerfällt also über $\mathbb{F}$ (es hat maximal p^n verschiedene Nullstellen) und daher ist ein Zerfällungskörper von f in $\mathbb{F}$ enthalten. Da f aber ein separables Polynom ist (endliche Körper sind perfekt), hat es genau p^n verschiedene Nullstellen und somit gibt es genau einen bis auf Isomorphie eindeutigen Körper mit p^n Elementen, nämlich den Zerfällungskörper $\mathbb{F}_{p^n}$ des Polynoms $X^{p^n} - X$.*

Frage 20 Was ist die Galois-Gruppe einer endlichen Erweiterung eines endlichen Körpers?

Antwort. *Es ist $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ eine Galoiserweiterung und daher $|Gal(\mathbb{F}_{p^n}, \mathbb{F}_p)| = n$. Für alle $i \in \{0, \ldots, n-1\}$ ist F^i in der Galoisgruppe. Der Frobenius Homomorphismus F hat Ordung n, da das Polynom $X^{p^m} - X$ für $0 < m < n$ nicht $|\mathbb{F}_{p^n}|$ Nullstellen haben kann. Also $Gal(\mathbb{F}_{p^n}, \mathbb{F}_p) = \mathbb{Z}_n = \langle F \rangle$. Es gilt also $\mathbb{F}_p^m \subseteq \mathbb{F}_p^n$ genau dann, wenn $m|n$, denn $\mathbb{Z}_n$ hat zu jedem Teiler m von n genau eine Untergruppe.*

Frage 21 Ist das Polynom $f = X^5 - 2X^3 - 8X - 2$ aus $\mathbb{Q}[X]$ auflösbar?

Antwort. *Nein (siehe Skript), denn ist $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit einem primen Grad p, so ist $Gal_{\mathbb{Q}}(f) = \Sigma_p$, falls f genau zwei komplexe Nullstellen hat (wieso?).*

Frage 22 Ist das Polynom $f = X^5 - X - 1$ aus $\mathbb{Q}[X]$ auflösbar?

Antwort. *Diese Antwort benutzt in der Vorlesung nicht behandelte Resultate. Das Polynom f hat nach dem Satz von den rationalen Nullstellen keine Nullstellen in $\mathbb{Q}$, denn wäre $\frac{a}{b}$ eine solche, dann $a|1$ aber $f(\pm 1) \neq 0$. Tatsächlich ist $f \in \mathbb{Z}[X]$. Modulo $p = 5$ ist $\bar{f}$ irreduzibel (wieso?), also ist f in $\mathbb{Q}[X]$ irreduzibel. Das Polynom f ist nicht auflösbar, wenn wir zeigen $\Sigma_5 \subseteq Gal_{\mathbb{Q}}(f)$. Dazu genügt es (wieso?), ein Element von Ordnung 5 und ein Element von Ordnung 6 in $Gal_{\mathbb{Q}}(f)$ zu finden. Ein Element von Ordung 5 haben wir schon gefunden, denn nach dem Satz von Cauchy (siehe Sylowsätze) gibt es zu jedem Primteiler p der Gruppenordung $|Gal_{\mathbb{Q}}(f)|$ auch ein Element der Ordung p in $Gal_{\mathbb{Q}}(f)$ und es teilt 5 die Zahl $|Gal_{\mathbb{Q}}(f)|$, da f irreduzibel ist. Interessant ist das folgende Lemma. Einen Beweis kann man z.B. in dem Algebra Buch von Serge Lang in VII.2.9. finden.*

Lemma 0.2 *Ist $f \in \mathbb{Z}[X]$ ein normiertes Polynom und p eine Primzahl, so ist $Gal_{\mathbb{F}_p}(\bar{f})$ isomorph zu einer Untergruppe von $Gal_{\mathbb{Q}}(f)$.*

Es gilt in $\mathbb{F}_2$, dass $\bar{f} = \bar{g}\bar{h} = (X^2 + X + 1)(X^3 + X^2 + 1)$ (dies kann man z.B. explizit durch Lösen einer Gleichung für die Koeffizienten sehen). Beide Faktoren sind irreduzibel, da $\bar{f}$ keine Linearfaktoren in $\mathbb{F}_2$ hat (Null und Eins einsetzen!). Ist a eine Nullstelle von $X^2 + X + 1$ und b eine Nullstelle von $X^3 + X^2 + 1$, so hat $\mathbb{F}_2 \subseteq \mathbb{F}_2(a, b)$ den Grad 6 (wieso?). Es ist $\mathbb{F}_2(a, b)$ auch der Zerfällungskörper von $\bar{f}$ (wieso?). Es gibt genau zwei Gruppen der Ordnung 6 nämlich $\mathbb{Z}_6$ und S_3, aber es ist $Gal_{\mathbb{F}_2}(\bar{f}) = \mathbb{Z}_6$, da die Galoisgruppe einen Normalteiler der Ordnung 2 enthalten muss. Nach dem Lemma enthält $Gal_{\mathbb{Q}}(f)$ also ein Element von Ordnung 6. Nach 20.3. ist $Gal_{\mathbb{Q}}(f) \subseteq \Sigma_5$ und Σ_5 wird von einem Element von Ordnung 5 zusammen mit einem Element von Ordnung 6 erzeugt (wieso?). Also ist das Polynom nicht auflösbar.