

Übungen zur Algebra I

- 9. Blatt -

Prof. Dr. K. Wingberg
J. Bartels

WS 2010/2011
abzugeben bis Donnerstag, den 16. Dezember 2010 um 9:15 Uhr
in den Kästen neben dem Seifertraum

<http://www.mathi.uni-heidelberg.de/~bartels/Vorlesung>

Name: /name/ Matrikelnummer: /nr/
Übungsleiter: /uebleiter/
2. Name: /namezwei/ 2. Matrikelnummer: /nrzwei/

Man achte auf eine saubere Darstellung und eine ordentliche Schrift.
Bitte keine maschinell erstellten Lösungen abgeben.

Aufgabe	1	2	3	4	Σ
Punkte					

Avant-Propos:

In der Vorlesung wurde die symmetrische Gruppe S_n behandelt, diese besitzt bemerkenswerte Elemente: die Zyklen σ der Ordnung k . Über diese sei die folgende Bemerkung gemacht - sie werden folgendermaßen notiert: $\sigma = (a_1, \dots, a_k)$, wobei die $a_i \in \{1, \dots, n\}$ paarweise verschieden sind. Dies bedeutet, daß $\sigma(a) = a$ gilt, wenn a nicht in den a_i auftaucht und ansonsten $\sigma(a_i) = a_{i+1}$ gilt, wobei der Index modulo k genommen wird. Ein solches Element aus S_n hat die Ordnung k (ausprobieren oder glauben!). Im Fall $k = 2$ spricht man von einer Transposition. Zwei Zyklen nennt man disjunkt, wenn kein a_i des einen ein a_i des anderen ist.

Des Weiteren nehme man das folgende hin:

0.0.1 Satz: Ist p eine Primzahl und f ein separables normiertes Polynom aus $\mathbb{Z}[X]$ vom Grad n . \bar{f} sei das modulo p reduzierte Polynom in $\mathbb{Z}/p\mathbb{Z}[X]$. Ist \bar{f} separabel und sei

$$\bar{f} = \prod_{1 \leq i \leq t} \bar{f}_i$$

die Zerlegung in irreduzible Faktoren $\bar{f}_i \in \mathbb{Z}/p\mathbb{Z}[X]$ vom Grad n_i . Dann gibt es t disjunkte Zyklen $(\sigma_i)_{1 \leq i \leq t}$ in S_n , jeweils der Ordnung n_i , so daß das Produkt $\prod_{1 \leq i \leq t} \sigma_i$ in $G(f, \mathbb{Q}) \subset S_n$ enthalten ist.

1 . Aufgabe (6 Punkte):

Der eingangs aufgeführte Satz verdeutlicht, wie sinnvoll es ist, ein Polynom modulo einer Primzahl zu zerlegen. Auf der gruppentheoretischen Seite ist es erforderlich, die verschiedenen Zykeltypen (Schreibweise: (n_1, \dots, n_t) , wobei $\sum_{1 \leq i \leq t} n_i = n$) zu kennen, welche in transitiv operierenden Untergruppen der S_n vorkommen.

Hierbei schreibt man die Zykeltypen so, daß stets $n_1 \leq n_2 \leq \dots \leq n_t$ gilt.

- a) Was für Galoisgruppen kann $f(X)$ über K überhaupt haben, wenn $f(X)$ irreduzibel vom Grad 4 ist? Welche Ordnungen haben sie? Gibt es eine größte Gruppe unter ihnen, in denen die anderen enthalten sind? Welche? Zeichnen Sie einen Untergruppengraphen, der verdeutlicht, welche Gruppe in welcher enthalten ist. Welche Zykeltypen kommen in diesen Gruppen wie oft vor?

Fertigen Sie eine Tabelle an, aus der dies klar ersichtlich wird.

Nota bene: Ein tiefliegender Satz der algebraischen Zahlentheorie - der Tschebotareffsche Dichtigkeitssatz besagt, daß jeder in $Gal(f, \mathbb{Q})$ auftretende Zykeltyp mit dem Zerlegungsverhalten modulo einer geeigneten Primzahl p übereinstimmt und wenn man bezüglich allen - immer größeren - Primzahlen reduziert, man die einzelnen Zykeltypen entsprechend ihrer Häufigkeit in $Gal(f, \mathbb{Q})$ auffinden wird.

2 . Aufgabe (6 Punkte):

Zeigen Sie mit Hilfe der 1. Aufgabe des 3. Blatts, daß jedes Polynom aus der Menge

$$\{X^4 + 27X^3 + X^2 + 13X + 17 + P(X) \mid P(X) \in 30\mathbb{Z}[X]\}$$

vom Grad 4 irreduzibel ist und $Gal(f, \mathbb{Q}) = S_4$ gilt. Benutzen Sie dazu auch die 2. Aufgabe des 4. Blatts.

3 . Aufgabe (6 Punkte):

Es sei $f(X) \in K[X]$ ein normiertes Polynom n -ten Grades mit Koeffizienten aus einem Körper K . Ω/K sei ein fest gewählter algebraischer Abschluß von K und $\{x_1, \dots, x_n\} \subset \Omega$ die Menge der Nullstellen von $f(X)$ in K .

- a) Zeigen Sie, daß für die Diskriminante $D(f)$ des Polynoms f gilt:

$$Gal(f, K) \leq A_n \Leftrightarrow D(f) \in K^2.$$

Nota bene: Die A_n ist die Untergruppe der geraden Permutationen in S_n .

- b) Ist die Galoisgruppe des Polynoms $X^6 - 1536X - 5120$ über \mathbb{Q} in der A_6 enthalten?
(**Hinweis:** letztes Blatt, 2. Aufgabe)

4 . Aufgabe (6 Punkte):

Es sei K ein Körper der Charakteristik 0.

- a) Ist $n = 4$ und $f(X)$ irreduzibel und durch $f(X) = X^4 + pX^2 + qX + r \in K[X]$ gegeben, dann ist für

$$z_1 := (x_1 + x_2)(x_3 + x_4)$$

$$z_2 := (x_1 + x_3)(x_2 + x_4)$$

$$z_3 := (x_1 + x_4)(x_2 + x_3)$$

das Polynom $Q(X) := \prod_{1 \leq i \leq 3} (X - z_i)$ ein Polynom aus $K[X]$. Hierbei seien x_1, \dots, x_4 die Nullstellen von f .

(Hinweis: 7. Blatt, 2. Aufgabe)

- b) Man zeige, daß

$$\text{Gal}(f, K) \leq D_4 \Leftrightarrow Q(X) \text{ ist reduzibel in } K(\sqrt{D(f)})[X]$$

gilt.

Nota bene: Die D_4 ist die Drehgruppe mit 8 Elementen, s. 2. Aufgabenblatt, 3. Aufgabe.

Nota bene: Die Gruppe aus der 4. Aufgabe des 7. Blatts heißt „*semidirektes*“ Produkt der Gruppen N und H , welches durch den Homomorphismus $\varphi : H \rightarrow \text{Aut}(N)$ gegeben ist. Im Fall abelscher Gruppen N und H ist dies der einfachste Fall einer Gruppe, welche a) N als Normalteiler b) H als Untergruppe und Quotient hat. Ein klassisches Beispiel, wo diese Gruppe auftaucht:

$$1 \rightarrow \text{Gal}(\mathbb{Q}(\sqrt[p]{p}, \zeta_q)/\mathbb{Q}(\zeta_q)) \rightarrow \text{Gal}(\mathbb{Q}(\sqrt[p]{p}, \zeta_q)/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \rightarrow 1.$$

Hierbei seien p, q zwei verschiedene Primzahlen und $q \not\equiv 1 \pmod{p}$. Desgleichen verhält es sich mit der Sequenz

$$1 \rightarrow SL_n(K) \rightarrow GL_n(K) \xrightarrow{\det} K^* \rightarrow 1$$

oder

$$1 \rightarrow A_n \rightarrow S_n \xrightarrow{\text{sign}} \{\pm 1\} \rightarrow 1.$$

Allgemein gilt für eine Sequenz

$$1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$$

beschreibt im Falle teilerfremder Ordnungen, also $(\#N, \#H) = 1$ ein (semi)direktes Produkt. Dies ist genau dann direkt, wenn $H \rightarrow \text{Aut}(N)$ der triviale Homomorphismus ist. Dieser Umstand ist Kernaussage des Satzes von Schur und Zassenhaus.

Nota bene 2: In der ersten Aufgabe desselben Blatts wurde der Hauptsatz über elementarsymmetrische Polynome behandelt. Er ist ein notwendiges Werkzeug zur systematischen Bearbeitung von Transzendenzfragen (e und π) und war eben auch in der zweiten Aufgabe dienlich gewesen.