Übungen zur Algebra I

- 10. Blatt -

Prof. Dr. K. Wingberg
J. Bartels

WS 2008/2009

abzugeben bis Dienstag, den 16. Dezember 2008 um 9:15 Uhr

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	$\sum$
Punkte					

Avant-Propos:
In der Vorlesung wurde die symmetrische Gruppe S_n behandelt, diese besitzt bemerkenswerte Elemente: die Zykel σ der Ordnung k. Über diese sei die folgende Bemerkung gemacht - sie werden folgendermaßen notiert: $\sigma = (a_1, ..., a_k)$, wobei die $a_i \in \{1, ..., n\}$ 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 Zykel 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. $\overline{f}$ sei das modulo p reduzierte Polynom in $\mathbb{Z}/p\mathbb{Z}[X]$. Ist $\overline{f}$ separabel und sei*

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

die Zerlegung in irreduzible Faktoren $\overline{f}_i \in \mathbb{Z}/p\mathbb{Z}[X]$ vom Grad n_i. Dann gibt es t disjunkte Zykel $(\sigma_i)_{1 \leq i \leq t}$ 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):
Zeigen Sie:

a) Wenn eine Untergruppe $G \leq S_n$ transitiv auf $\{1, ..., n\}$ operiert und eine Transposition und einen Zykel der Länge $n-1$ enthält, gilt $G = S_n$.

b) Es sei G eine transitive Untergruppe von S_n und enthalte einen p-Zyklus $\sigma = (1, 2, ..., p)$ und eine Transposition (i, j), wobei p eine Primzahl $> \frac{n}{2}$ ist. Dann ist $G = S_n$.

c) Was bedeutet das im Hinblick auf die Galoisgruppe eines normierten Polynoms vierten Grads aus der Menge $(X^4 + 5X^3 + 17X^2 + 15X + 17) + 30\mathbb{Z}[X]$ (s. 5. Blatt, 2. Aufgabe)?

d) Geben Sie unter Benutzung von a) ein Polynom vierten Grades an, dessen Galoisgruppe die S_4 ist.

2 . Aufgabe (6 Punkte):
Es sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, y)$ mit $y^2 = (9 - 5\sqrt{3})(2 - \sqrt{2})$. Zeigen Sie:

a) $K/\mathbb{Q}$ ist galoissch.

b) $Gal(K/\mathbb{Q}) = Aut(K/\mathbb{Q}) \cong G$,
wobei G die Gruppe aus 8 Elementen aus dem 6. Blatt, 3. Aufgabe ist.

3 . 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: $(n_1, ..., n_t)$, 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 $n_1 \leq n_2 \leq ... \leq n_t$ gilt.

a) Auf dem 9. Blatt, 4. Aufgabe haben Sie die 5 transitiven Untergruppen der S_4:

$$S_4, A_4, D_4, Z_4(\cong \mathbb{Z}/4\mathbb{Z}), V_4(\cong (\mathbb{Z}/2\mathbb{Z})^2)$$

kennengelernt. Welche Zykeltypen kommen in diesen Gruppen wie oft vor?
Fertigen Sie eine Tabelle an, aus der dies klar ersichtlich wird.

b) Was ist die Galoisgruppe des Polynoms $f(X) = X^4 + 3X^2 + 7X + 4 \in \mathbb{Q}[X]$?

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.

4 . Aufgabe (6 Punkte):
Es sei $n \in \mathbb{N}$ und p eine Primzahl. Man zeige:

a) $Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$, wobei $\zeta_{p^n} := e^{\frac{2\pi i}{p^n}} \in \mathbb{C}$ ist.
Hinweis: Überlegen Sie sich, auf welche Elemente aus $\mathbb{Q}(\zeta_{p^n})$ die Größe ζ_{p^n} abgebildet werden darf.

b) Es gibt eine galoissche Erweiterung K von $\mathbb{Q}$, so daß $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ ist. (wem es gefällt: o.B.d.A. sei n ungerade). Hinweis: Man zerlege n in Primfaktoren und nutze das 8. Blatt, 4. Aufgabe.

Nota bene: Man nennt Erweiterungen, die durch Adjunktion von Einheitswurzeln entstehen, Kreisteilungserweiterungen. Ein tiefliegender Satz der Algebraischen Zahlentheorie - der Satz von Kronecker-Weber - besagt, daß jede abelsche Erweiterung von $\mathbb{Q}$ - d.h. jede Galoiserweiterung mit abelscher Galoisgruppe - in einem Kreisteilungskörper enthalten ist.

Zusätzliche Fragen zum letzten Zettel (ohne Wertung)

a) Vergleicht man die Methode der Galoisgruppenbestimmung des letzten Zettels mit der dieses Zettels, was kann man dazu sagen?

b) Wenn das Polynom der vierten Aufgabe fünften Grads gewesen wäre, was für Gruppen wären dann in Frage gekommen?

Nota bene:
Die dritte Aufgabe des letzten Zettels steht in allgemeinerem Zusammenhang. Grundsätzlich ist zu sagen, daß für gerade $n \in \mathbb{N}_{\leq 50}$ Polynome der Form

$$X^n - n^{n-1}X + n^{n-1}(n-1) \text{ im Fall } 4|n$$

und

$$X^n - n(2-n)^{n-2}X + (2-n)^{n-1}(n-1) \text{ im Fall } 4 \not| n$$

als Galoisgruppe A_n haben. Ausführlicher kann man fragen: Gibt es zu einer gegebenen endlichen Gruppe ein Polynom (über K), welches diese Gruppe als Galoisgruppe hat? Über $\mathbb{C}(X)$ ist sie positiv beantwortet, über $\mathbb{Q}$ steht eine Antwort aus. In den letzten 20-30 Jahren haben sich viele Menschen darüber Gedanken gemacht, wie dies Problem anzugehen sei, u.a. waren unsere Kollegen im IWR gegenüber dabei sehr erfolgreich. Mehr dazu in: Topics in Galois Theory von J.-P. Serre oder in jedem anderen Buch über Inverse Galoistheorie. (Invers deswegen, da man nicht von der Gleichung zur Gruppe übergeht, sondern es eben andersherum probiert.)
Nota bene 2:
Ist K ein Körper und nimmt man die endlich-dimensionalen zentralen Schiefkörper L/K, d.h. endlich-dimensionale, nicht-kommutative Erweiterungen L von K, deren Zentrum K selbst ist, und teilt sie in Ähnlichkeitsklassen ein, dann kann man auf diesen Klassen mit Hilfe des Tensorprodukts über K eine Gruppenstruktur feststellen. Das heißt, das Produkt gutartiger Schiefkörper über einem Grundkörper liefert in kanonischer Weise einen weiteren Schiefkörper - welcher allerdings nur durch das Tensorprodukt definiert wird, ihm jedoch nicht exakt entspricht. Mehr dazu in M. Deuring: Algebren oder F. Lorenz: Algebra II; dies ist jedoch nicht Inhalt der Vorlesung im kommenden Semester.
Nota bene 3:
Die semidirekten Produkte aus dem 8. Blatt stellen - neben den direkten Produkten - die einfachste Art Gruppe dar, die über einen gegebenen Normalteiler und gegebenen Quotienten verfügen. Allgemein sieht die Welt häßlicher aus und wird durch sog. Faktorensysteme beschrieben, die wiederum die zweite Kohomologiegruppe $H^2(G/N, N)$ (andere nennen sie Brauergruppe) darstellen. Der Oberbegriff dazu heißt Gruppenerweiterungstheorie und entstammt der folgenden Fragestellung: Gegeben seien galoissche Erweiterungen L/K und K/k. Wenn L/k galoissch ist - das ist nicht unbedingt der Fall, s. Hauptsatz der Galoistheorie! - , welche Gruppe kann diese Erweiterung haben? Behandelt wird dies in Huppert: Endliche Gruppen oder in anderem Zusammenhang in J. Neukirch, A. Schmidt, K. Wingberg: Cohomology of Number Fields.