Übungen zur Algebra I

- 3. Blatt -

Prof. Dr. K. Wingberg
J. Bartels
.

WS 2010/2011

abzugeben bis Donnerstag, den 4. November 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	$\sum$
Punkte					

---

1 . Aufgabe (6 Punkte):
Es sei $U \subseteq S_n$ eine Untergruppe der symmetrischen Gruppe S_n. Zeigen Sie:

a) Wenn ein $(n-1)-$Zykel $(a_1 \ \cdots \ a_{n-1})$ und eine Transposition $(a_i \ a_j)$ in U enthalten ist und es für alle $i, j \in \{1, ..., n\}$ ein Element $u \in U$ gibt, so daß $u(i) = j$ ist, dann ist $U = S_n$.

b) Es sei p eine Primzahl, welche größer als $\frac{n}{2}$ ist. Wenn ein $p-$Zykel $(a_1 \ \cdots \ a_p)$ und eine Transposition $(a_i \ a_j)$ in U enthalten ist und es für alle $i, j \in \{1, ..., n\}$ ein Element $u \in U$ gibt, so daß $u(i) = j$ ist, dann ist $U = S_n$.

2 . Aufgabe (6 Punkte):
Es sei der Körper $\mathbb{F}_2$ und das Polynom $f(X) := X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ gegeben.

a) Zeigen Sie, daß $f(X)$ ein über $\mathbb{F}_2$ irreduzibles Polynom darstellt.

b) Finden Sie einen Erzeuger der multiplikativen Gruppe des Körpers $\mathbb{F}_2[X]/(f(X))$.

3 . Aufgabe (6 Punkte):
Diese Aufgabe beschäftigt sich mit der expliziten Faktorisierung von Polynomen.
Es sei $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ gegeben.

a) Zeigen Sie, daß wenn es einen Teiler $t(X)$ von $f(X)$ gibt, d.h. $f(X) = s(X)t(X)$ mit $s(X), t(X) \in \mathbb{Z}[X]$, dann gilt o.E: $m := Grad(t(X)) \leq \frac{1}{2}n$. Wenn man mit $z_0, ..., z_m$ paarweise verschiedene ganze Zahlen nimmt, welche Werte kann $t(z_i)$ mit $i \in \{0, ..., m\}$ nur annehmen?

b) Man folgere, daß das Polynom in endlich vielen Schritten faktorisierbar ist. D.h. unter anderem, daß man in endlich vielen Schritten feststellen kann, ob ein Polynom in $\mathbb{Z}[X]$ reduzibel ist oder nicht. (Hinweis: Lagrange-Interpolation)

4 . Aufgabe (6 Punkte):
Es sei p eine Primzahl $\neq 2$ und $n \in \mathbb{N}$

a) Zeigen Sie, daß für die multiplikative Gruppe $(\mathbb{Z}/p^n\mathbb{Z})^*$ gilt

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

(Hinweis: Betrachten Sie die Ordnung des Elements $(1+p)$.)

b) Wie könnte der Fall $p = 2$ aussehen? Gilt diese Formel dann auch?