HUMBOLDT–UNIVERSITÄT ZU BERLIN
Mathematisch-Naturwissenschaftliche Fakultät II
Institut für Mathematik
Prof. Dr. U. Kühn

Humboldt-Universität zu Berlin, Institut für Mathematik, Rudower Chaussee 25, 12489 Berlin

Übungsaufgaben zur Vorlesung Algebra 1

Serie 6. Abgabetermin: 27.5.05

Aufgabe 1 (3 Punkte):

(a) Finde die kleinste Zahl $x \in \mathbb{N}$ mit $x \equiv 3 \mod 4$, $x \equiv 1 \mod 9$ und $x \equiv 4 \mod 5$.

(b) Man berechne den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von 17201 und 13861.

(c) Man berechne mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der folgenden Polynome aus $\mathbb{Q}[x]$:

$$f = x^3 + x^2 + x - 3, \quad g = x^6 - x^5 + 6x^2 - 13x + 7.$$

Aufgabe 2 (4 Punkte):

(a) Man zeige, dass $\mathbb{Z}[i] = \{x + iy \in \mathbb{C} \,|\, x, y \in \mathbb{Z}\} \subset \mathbb{C}$ versehen mit der Normabbildung $\delta : \mathbb{Z}[i] \to \mathbb{N}$ gegeben durch $\delta(x + iy) = x^2 + y^2$ ein euklidischer Ring ist.

(b) Man berechne den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von $1 + 7i$ und $6 + 17i$.

Aufgabe 3 (4 Punkte): Gegeben sei der Unterring $R = \mathbb{Z} + \sqrt{-5}\mathbb{Z} \subset \mathbb{C}$.

(a) Man zeige, das Ideal $(2, 1 + \sqrt{-5}) \subset R$ ist ein Primideal das nicht von einem Element erzeugt werden kann.

(b) Man beweise, dass R ist nicht faktoriell ist. Tip: Betrachte die Faktorisierungen $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ und zeige, dass die Elemente 2, 3, $1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ jeweils irreduzibel und paarweise nicht assoziert sind.

Aufgabe 4 (4 Punkte): Sei R ein Unterring eines Ringes R'. Für $\alpha \in R'$ betrachte man den Einsetzungshomomorphismus $\varphi_\alpha : R[x] \to R'$ gegeben durch $\varphi_\alpha(f(x)) = f(\alpha)$. Man beschreibe den Kern und das Bild von φ_α. Wann ist $\ker(\varphi_\alpha)$ ein Primideal bzw. ein maximales Ideal in $R[x]$?

Aufgabe 5 (20.000* Punkte): Man bestimme die Primfaktorzerlegung von folgender 193-stelligen RSA-Zahl:
3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609.

phone: 030/2093-5412 fax: 030/2093-5853 e-mail: kuehn@mathematik.hu-berlin.de
grabitz@mathematik.hu-berlin.de http://www.mathematik.hu-berlin.de/~kuehn/uebungen.html