XIV. ÜBUNG zu GRUNDZÜGE der ALGEBRA

Abgabe: MI, 7. FEB. 2007, 11:00 UHR in den orangen Kasten Nr. **8**

`http://math-www.upb.de/~dirk/Vorlesungen/GZ-Algebra/`

Bitte geben Sie außer Ihrem Namen auch **deutlich** die Übungsgruppe mit an.

Klausurtermin: Montag, 12.2.2007, 9:00 - 12:00 Uhr im Hörsaal C1.

42. Aufgabe: Bob möchte chiffrierte Nachrichten empfangen können. Dazu bastelt er sich zwei Schlüssel, einen öffentlichen und einen geheimen. Er wählt zwei Primzahlen $p = 23$ und $q = 29$ und setzt $n = p \cdot q = 667$. Er wählt dann $e = 575$ und setzt den öffentlichen Schlüssel ($n = 667$, $e = 575$) in ein öffentliches Schlüsselverzeichnis.

a) Wie muss er d für den geheimen Schlüssel (n, d) wählen?

b) Alice möchte Bob eine kurze Nachricht (hier: $x = 3$) geheim übermitteln. Sie entnimmt Bobs Schlüssel dem Verzeichnis. Wie sieht die verschlüsselte Nachricht aus?

c) Man zeige, wie Bob die empfangene Nachricht wieder entschlüsselt. 10 P.

43. Aufgabe: Sei R ein Integritätsbereich. Man zeige, dass R faktoriell ist *genau dann*, wenn sich jede von 0 verschiedene Nichteinheit von R in ein Produkt von endlich vielen irreduziblen Elementen zerlegen lässt, und diese irreduziblen Elemente bis auf Reihenfolge und Assoziiertheit eindeutig sind. 10 P.

44. Aufgabe: Sei R ein Hauptidealring und $p \in R$ ein Primelement. Man zeige: Der Faktorring R/pR ist ein Körper. 10 P.