Übungen zur Algebra I, SS 2002

Abgabe am Dienstag, den 11.06.2002 vor der Vorlesung

Aufgabe 25. *(Einheitengruppe von $\mathbb{Z}$, Eulersche φ-Funktion)*
Für eine natürliche Zahl n definieren wir $\varphi(n)$ als die Anzahl der zu n teilerfremden natürlichen Zahlen kleiner als n. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ nennt man *Eulersche φ-Funktion.*

a) Zeigen Sie, dass gilt: $\mathbb{Z}_n^* = \{\, m + n\mathbb{Z} \in \mathbb{Z}_n \mid \mathrm{ggT}(m,n) = 1 \,\}$
und folgern Sie: $|\mathbb{Z}_n^*| = \varphi(n)$.

b) Zeigen Sie, dass für teilerfremde natürliche Zahlen m und n gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \ .$$

(Hinweis: Nutzen Sie den bekannten Isomorphismus $\mathbb{Z}_{m \cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.)

c) Sei $p_1^{n_1} \cdot \dots \cdot p_r^{n_r}$ die Primfaktorzerlegung von n ($p_i \neq p_j$ für $i \neq j$). Zeigen Sie:

$$\varphi(n) = p_1^{n_1 - 1} \cdot \dots \cdot p_r^{n_r - 1} \cdot (p_1 - 1) \cdot \dots \cdot (p_r - 1) \ .$$

(Hinweis: Beweisen Sie die Aussage zunächst für $n = p_1^{n_1}$ mit nur einer Primzahl p_1.)

Aufgabe 26. *(Chinesischer Restsatz)*
Lösen Sie die folgenden simultanen Kongruenzen:

a)
$$\begin{aligned} x &\equiv 14 \mod 3 \ , \\ x &\equiv 4 \mod 10 \ . \end{aligned}$$

b)
$$\begin{aligned} y &\equiv 2 \mod 3 \ , \\ y &\equiv 4 \mod 8 \ , \\ y &\equiv 6 \mod 11 \ , \\ y &\equiv 8 \mod 35 \ . \end{aligned}$$

Aufgabe 27. *(Ideale und Homomorphismen)*
Seien R und S Ringe, I ein Ideal in R und $f : R \to S$ ein surjektiver Ringhomomorphismus.

a) Es sei $M_1 := \{\,\text{Ideale } I \text{ in } R \text{ mit } \mathrm{kern} f \subset I\,\}$ und $M_2 := \{\,\text{Ideale in } S\,\}$.
Geben Sie eine bijektive Abbildung zwischen M_1 und M_2 an, und folgern Sie, dass die Ideale in R/I 1:1 korrespondieren zu den Idealen J in R mit $I \subset J$.

b) Seien nun $P \subset R$, $Q \subset S$ Primideale mit $\mathrm{kern} f \subset P$ und $M \subset R$, $N \subset S$ maximale Ideale mit $\mathrm{kern} f \subset M$. Welche Eigenschaften (Primideal, maximales Ideal) besitzen $f(P)$ und $f(M)$ beziehungsweise $f^{-1}(Q)$ und $f^{-1}(N)$?