Übungsaufgaben zur Algebra

1. *(4 Punkte)* (Ein Beispiel ähnlich zu 7.28 in der Vorlesung)
   (a) Zeigen Sie, daß im Ring $\mathbb{Z}[\sqrt{5}] = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{5} \subset \mathbb{C}$ die Elemente 2, $3 + \sqrt{5}$ und $3 - \sqrt{5}$ irreduzibel sind und daß sie paarweise nicht assoziiert sind.
   (b) Begründen Sie (bitte etwas ausführlicher als in 7.28), daß aus (a) und aus
   $$2 \cdot 2 = 4 = (3 + \sqrt{5}) \cdot (3 - \sqrt{5})$$
   folgt, daß 4 nicht eindeutig (bis auf Multiplikation mit Einheiten) in irreduzible Faktoren zerlegbar ist, daß 2, $3 + \sqrt{5}$ und $3 - \sqrt{5}$ keine Primelemente sind und daß $\mathbb{Z}[\sqrt{5}]$ kein ZPE-Ring ist.
2. *(3 Punkte)* Bestimmen Sie für alle $d \in \mathbb{Z}$ mit $d < 0$ und d kein Quadrat die Einheitengruppen $(\mathbb{Z}[\sqrt{d}])^*$.
   Hinweise: (i) mit 7.27. (ii) Es gibt wenige Einheiten.
3. *(2+1 Punkte)*
   (a) Beweisen Sie die folgende Verallgemeinerung des kleinen Satzes von Fermat:
   Es seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(m, a) = 1$. *Dann gilt*
   $$a^{\varphi(m)} \equiv 1 \mod m.$$
   (b) Folgern Sie: *Es seien p und q zwei verschiedene Primzahlen, $a \in \mathbb{Z}$ und $r \in \mathbb{N} \cup \{0\}$. Dann gilt*
   $$a^{1+r(p-1)(q-1)} \equiv a \mod pq.$$
4. *(3 Punkte)* Es sei $(p_1, p_2, p_3) = (7, 11, 13)$ und
   $$(a_{ij})_{i=1,2,3;j=1,2,3,4} = \begin{pmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 6 \end{pmatrix}.$$
   Sehen Sie sich den Beweis der klassischen Version des chinesischen Restsatzes (8.1 in der Vorlesung) an und bestimmen Sie für $j = 1, 2, 3, 4$ Zahlen $x_j \in \{0, 1, ..., 7 \cdot 11 \cdot 13 - 1\}$ mit den Eigenschaften
   $$x_j \equiv a_{ij} \mod p_i \qquad \text{für } i = 1, 2, 3.$$
   Führen Sie genügend Zwischenschritte aus, so daß klar ist, daß Sie allein mit Papier und Bleistift gerechnet haben.
5. *(3 Punkte)* Nach Satz 8.6 der Vorlesung hat läßt sich jede endliche abelsche Gruppe in der Gestalt
   $$\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}} \times .. \times \frac{\mathbb{Z}}{p_s^{\alpha_s}\mathbb{Z}}$$
   mit $p_1, ..., p_s$ Primzahlen (evtl. $p_i = p_j$) und auch in der Gestalt
   $$\frac{\mathbb{Z}}{b_1\mathbb{Z}} \times .. \times \frac{\mathbb{Z}}{b_k\mathbb{Z}}$$
   mit $b_1, ..., b_k \in \mathbb{N} - \{1\}$ und $b_i | b_{i+1}$.
   Geben Sie ohne Beweis für alle abelschen Gruppen der Ordnung 720 in einer Tabelle die beiden Tupel $(p_1^{\alpha_1}, ..., p_s^{\alpha_s})$ und $(b_1, ..., b_k)$ an.

Alle Informationen zur Vorlesung (Termine, Übungsblätter, Skript etc.) sind unter

`http://hilbert.math.uni-mannheim.de/Algebra05-06.html`

zu finden.

Abgabe bis Mittwoch, den 11. Januar 2006, vor der Vorlesung in A5.