Einführung in die Algebra
Prof. Dr. Günter Pilz
Übungsaufgaben 4, May 6th

1)

Prove Theorem 12.17 from the script.

2)

Prove Theorem 12.19 from the script (fill in all the missing details in the given proof).

3)

Find all abelian groups with order 360 up to isomorphism.

4)

Prove Theorem 14.1 (fill in all the details in the proof from the script).

5)

Let (5,551) be the public key and (101,551) be the private key of an RSA cryptosystem. Are those numbers validly chosen? If so, encrypt the message[351] and decrypt it afterwards. Could you crack this particular code?

6)

Let p = 72997 (a prime). Choose a "general key" S such that only 4 or more people have access to a secret storage facility Area 51. The participants C, F, H and P receive the "subkeys" f(1)=2022, f(3) = 10140, f(7)=51168, f(11)=53215. Find the general key. (Note: C, F, H and P do not know their codes 2022, … respectively).

7)

Show that $x^m - 1 | x^n - 1$ if and only if $m|n$.

8)

(a) Find $(1 + x^2 + x^4 + x^6 + \ldots)^{-1}$ in ($\mathbb{R}$[[x]], •).

(b) Under what conditions is a formal power series in ($\mathbb{Z}_p$[[x]], •) invertible? In ($\mathbb{R}$[[x]], •)?