

November 2, 2006

### 3rd Exercise Sheet Linear Algebra I for MCS Winter Term 2006/2007

#### (E3.1) [Isomorphisms]

Let  $(A, *^A, e^A)$  and  $(B, *^B, e^B)$  two structures with a binary operation and a distinguished element. Let  $\varphi : A \rightarrow B$  be a bijective map such that

$$\begin{aligned} \text{for all } x, y \in A : \quad & \varphi(x *^A y) = \varphi(x) *^B \varphi(y) \\ \text{and} \quad & \varphi(e^A) = e^B. \end{aligned}$$

Prove that  $(A, *^A, e^A)$  is a group if and only if  $(B, *^B, e^B)$  is a group.

#### (E3.2) [Groups and finite fields]

- (i) Let  $p$  be a prime. Show that for any integer  $a$  not divisible by  $p$  there is an integer  $k$  such that  $ka = 1 \pmod p$ . (Hint: recall from the OWO lecture that  $\gcd(s, t)$  can be expressed as an integer linear combination of  $s$  and  $t$ .)
- (ii) Let  $p$  again be prime. Show that in case  $p$  divides the product  $ab$  of two integers  $a$  and  $b$ , it must divide  $a$  or  $b$ .
- (iii) Let  $n$  be a positive integer. Show that  $(\mathbb{Z}_n \setminus \{0\}, \cdot_n, 1)$  is a group iff  $n$  is prime.

#### (E3.3) [Group theory]

- (i) Which of the following groups are isomorphic?
  - 1)  $(\mathbb{Z}_2^2, +, \mathbf{0})$
  - 2)  $(\mathbb{Z}_4, +, 0)$
  - 3)  $(\mathbb{Z}_5 \setminus \{0\}, \cdot, 1)$
  - 4)  $(\{x \in \mathbb{C} : x^4 = 1\}, \cdot, 1)$
  - 5)  $(\{x \in \mathbb{Z}_8 : 4x = 0\}, +, 0)$
- (ii) Find (up to isomorphism) all groups that have exactly 4 elements.  
(Hint: Analyse the possible choices by looking at the tables for the group operation and making suitable case distinctions when there are choices.)

**(E3.4) [Rings and fields]**

Let  $(R, +, \cdot, 0, 1)$  be a ring. Prove that

- (i)  $0 = 1$  if and only if  $R = \{0\}$ ,
- (ii) if  $R$  is a field then  $a \cdot b = 0$  implies  $a = 0$  or  $b = 0$ <sup>1</sup>.

**(E3.5) [Abelian groups and isomorphisms]**

Let  $(G, *, e)$  a group and  $\alpha : G \rightarrow G, g \mapsto g'$ , where  $g * g' = e$ . Show that  $\alpha$  is an isomorphism if and only if  $G$  is abelian.

---

<sup>1</sup>This shows that a field has now *zero divisors* and is a so-called *integral domain*.