

---

**ALGEBRA 2**  
**ÜBUNGSBLATT 4**

---

- (1) Consider  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}[i]$ . We showed last week, using the norm function, that  $\mathbb{Z}[i]$  is a UFD.

You may use without proof that for a prime number  $p$ , we have that

$$p \equiv 1 \pmod{4} \iff p = a^2 + b^2, \quad \text{for some } a, b \in \mathbb{Z}.$$

Prove the following:

- (a) The norm function is multiplicative.
  - (b) The extension of a prime ideal along  $\varphi$  may not be prime.
  - (c) If  $p \equiv 1 \pmod{4}$  then  $(p)^e$  is the product of two distinct prime ideals.
  - (d) If  $p \equiv 3 \pmod{4}$  then  $(p)^e$  is prime in  $\mathbb{Z}[i]$ .
- (2) Consider a ring  $A$  such that for every  $x \in A$  it holds that  $x^2 = x$ . Prove
- (a)  $2x = 0$  for every  $x \in A$ ;
  - (b) every prime ideal  $\mathfrak{p}$  is maximal and  $A/\mathfrak{p}$  is a field with two elements;
  - (c) every finitely generated ideal is principal.
- Suppose now that  $A$  is such that for every  $x \in A$  we have  $x^n = x$ . Prove that every prime ideal  $\mathfrak{p}$  is maximal. Prove that  $A/\mathfrak{p}$  is a finite field and find a bound for the number of elements.

- (3) Consider an exact sequence of  $A$ -modules

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0.$$

Show that if  $M'$  and  $M''$  are finitely generated, then so is  $M$ . Does the converse hold?

- (4) Let  $A$  be a ring and  $\mathfrak{a}$  be an ideal contained in the Jacobson radical of  $A$ . Moreover, let  $M$  be an  $A$ -module,  $N$  be a finitely generated  $A$ -module, and  $u : M \rightarrow N$  be  $A$ -linear. Show that if the induced map  $M/\mathfrak{a}M \rightarrow N/\mathfrak{a}N$  is surjective, then  $u$  is surjective.

(5) Let  $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  be an exact sequence of  $A$ -modules. Show that the following two conditions are equivalent.

(a) There is a morphism  $s : M'' \rightarrow M$  such that  $gs = \text{id}_{M''}$ .

(b) There is a morphism  $p : M \rightarrow M'$  such that  $pf = \text{id}_{M'}$ .

If these conditions hold, we say that the sequence splits. Show that in this situation, we have

$$M = \text{im}(s) \oplus \ker(g) = \text{im}(f) \oplus \ker(p) \cong M' \oplus M''.$$