

1. (Textbook 3.4)  
(Decide irreducibility of five polynomials)
2. (Textbook 3.5)  
(Decide irreducibility of three polynomials)
3. (Textbook 3.12)  
(Some true/false questions about factoring polynomials)
4. Prove, as claimed in class, that if  $\nu$  is a discrete valuation on a field  $K$ , and  $a, b \in K$  have  $\nu(a) \neq \nu(b)$ , then  $\nu(a + b) = \min\{\nu(a), \nu(b)\}$ .
5. Let  $\nu$  be a discrete valuation on a field  $K$ . Extend  $\nu$  from  $K$  to  $K[t]$  with the following definition:

$$\nu(a_0 + a_1t + \cdots + a_d t^d) = \min\{\nu(a_0), \nu(a_1), \dots, \nu(a_d)\}.$$

Prove that for all  $f, g \in K[t]$ ,  $\nu(fg) = \nu(f) + \nu(g)$ . **There was a misprint here originally: this should read  $\nu(f) + \nu(g)$ , not  $\nu(f)\nu(g)$ .**

**Hint** First, prove that  $\nu(fg) \geq \nu(f) + \nu(g)$ . Then, to show that equality holds, it suffices to exhibit a single coefficient with the desired valuation.

6. Let  $\alpha \in \mathbb{C}$  be an algebraic number, with minimal polynomial  $m \in \mathbb{Q}[t]$ . Let  $d = \deg_{\mathbb{Q}}(\alpha)$ , which we have seen is also equal to  $\partial m$ .
  - (a) Prove that  $m$  is *separable*, as defined in the previous problem set, and therefore has  $d$  distinct roots.
  - (b) Let  $\alpha_1, \dots, \alpha_d \in \mathbb{C}$  be the distinct roots of  $m$ ; as mentioned in class, these are called the *conjugates* of  $\alpha$ . Prove that all the conjugates  $\alpha_i$  have the same minimal polynomial  $m$ .
  - (c) Denote by  $N_{\mathbb{Q}}(\alpha)$  the product of all the conjugates, i.e.  $\alpha_1\alpha_2 \cdots \alpha_d$ . Prove that  $N_{\mathbb{Q}}(\alpha) \in \mathbb{Q}$ .
  - (d) Determine a formula for  $N_{\mathbb{Q}}(a + b\sqrt{d})$ . Here, assume  $a, b, d \in \mathbb{Z}$ ,  $d$  is squarefree, and  $b \neq 0$ .
7. Using the same notation as the previous problem:
  - (a) Prove that for each conjugate  $\alpha_i$ , there is a unique field homomorphism  $\phi_i : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$  such that  $\phi_i(\alpha) = \alpha_i$ .

**Hint** Use the isomorphism  $\mathbb{Q}(\alpha) \cong \mathbb{Q}[t]/\langle m \rangle$ , and apply the first isomorphism theorem for rings to reduce the problem to classifying certain homomorphisms  $\mathbb{Q}[t] \rightarrow \mathbb{C}$ .

- (b) Prove that in any nonzero field homomorphism  $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ ,  $\phi(\alpha)$  must be one of the conjugates of  $\alpha$ . Conclude that there exist exactly  $d$  nonzero homomorphisms  $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ .

**Note** This is yet possible way to define the degree of an algebraic number, and another point of view on “conjugates:” they are other avatars of  $\alpha$  under different choices of embedding of  $\mathbb{Q}(\alpha)$  in  $\mathbb{C}$ .