

Math 568 Homework 2
Spring 2009
Due: Thursday, January 29

1. Let m be a squarefree integer $\neq 0, 1$. Show that the ring of algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ is given by

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \quad \text{if } m \equiv 2 \text{ or } 3 \pmod{4},$$

and

$$\left\{ \frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\} \quad \text{if } m \equiv 1 \pmod{4}.$$

2. Show that $\mathbb{Z}[\sqrt{5}]$ is not integrally closed, and deduce that it cannot be a unique factorization domain. Give an example of an element of $\mathbb{Z}[\sqrt{5}]$ that has two distinct factorizations into irreducible elements.
3. Let A be an integrally closed ring, and let K be its field of fractions. Let $f(X) \in A[X]$ be a monic polynomial. If $f(X)$ is reducible in $K[X]$, show that it is reducible in $A[X]$.
4. Let A be a subring of a ring B , and let β be a unit in B . Show that every $\alpha \in A[\beta] \cap A[\beta^{-1}]$ is integral over A .
5. Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$, and let α be an algebraic integer in K . This exercise will show that the ring of algebraic integers \mathcal{O}_K in K does not equal $\mathbb{Z}[\alpha]$.

(a) Consider the four algebraic integers:

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10});$$

$$\alpha_2 = (1 + \sqrt{7})(1 - \sqrt{10});$$

$$\alpha_3 = (1 - \sqrt{7})(1 + \sqrt{10});$$

$$\alpha_4 = (1 - \sqrt{7})(1 - \sqrt{10}).$$

Show that all the products $\alpha_i\alpha_j$, $i \neq j$, are divisible by 3 in \mathcal{O}_K , but that 3 does not divide any power of any α_i . [Hint: Show that $\alpha_i^n/3$ is not an algebraic integer by considering its trace: show that $T(\alpha_i^n) \equiv (\sum \alpha_j^n) \equiv 4^n \pmod{3}$ in $\mathbb{Z}[\alpha]$; deduce $T(\alpha_i^n) \equiv 1 \pmod{3}$ in \mathbb{Z} .]

- (b) Assume now that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. We will derive a contradiction from this. Let $f(X)$ be the minimal polynomial of α over \mathbb{Q} . For $g(X) \in \mathbb{Z}[X]$, let $\bar{g}(X)$ denote the image of g in $\mathbb{F}_3[X]$. Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ if and only if \bar{g} is divisible by \bar{f} in $\mathbb{F}_3[X]$.
- (c) For each i , $1 \leq i \leq 4$, let f_i be a polynomial in $\mathbb{Z}[X]$ such that $\alpha_i = f_i(\alpha)$. Show that $\bar{f} \mid \bar{f}_i\bar{f}_j$, $i \neq j$, in $\mathbb{F}_3[X]$, but that \bar{f} does not divide \bar{f}_i^n for any n . Conclude that for each i , \bar{f} has an irreducible factor which does not divide \bar{f}_i , but does divide all \bar{f}_j , $j \neq i$.
- (d) This shows that \bar{f} has at least four distinct irreducible factors over \mathbb{F}_3 . On the other hand, f has degree at most 4. Why is this a contradiction?