

1. Let  $f(x) = x^3 + 3x^2 + 3x - 1 \in \mathbb{Q}[x]$ .

- (a) Find the remainder of  $x^4$  when divided by  $f(x)$ .
- (b) Find the remainder of  $(x^2 + 1)^3$  when divided by  $f(x)$ .
- (c) Find polynomials  $u(x), v(x) \in \mathbb{Q}[x]$ , with  $\deg(u(x)) \leq 2$  which solve

$$x^2 \cdot u(x) + v(x)f(x) = 1.$$

2. Let  $\alpha$  be the real number  $\alpha = 2^{1/3} - 1$ . To as many decimal places as you can (well, at least 8, and no more than 20), evaluate the following real numbers:

- (a)  $\alpha^4$ ;
- (b)  $(\alpha^2 + 1)^3$ ;
- (c)  $1/\alpha^2$ ;
- (d)  $3\alpha^2 + 10\alpha + 12$ ;
- (e)  $24\alpha^2 + 60\alpha - 16$ ;
- (f)  $6\alpha^2 + 10\alpha - 3$ .

Now,

- (g) explain why some of the numbers this question were the same (question 1 may help).

3. In this question we will show that  $f(x) = x^4 - 10x^2 + 1$  is the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ . Let  $q(x) \in \mathbb{Q}[x]$  be the (at the moment unknown) minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ . It is easy to check that  $f(\sqrt{2} + \sqrt{3}) = 0$ , which implies that  $q(x) \mid f(x)$ . To show that  $q(x) = f(x)$  we may therefore show either that  $f(x)$  is irreducible in  $\mathbb{Q}[x]$  or that  $\deg(q(x)) = 4$ .

We will use equality  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , proved in the last homework assignment to show that  $\deg(q(x)) = 4$ .

- (a) Using the chain of field extensions  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$  explain why  $\deg(q(x))$  must be even.

Since  $\deg(q(x)) \leq 4$ , this means that we must have  $\deg(q(x)) = 2$  or  $4$ . We now assume that  $\deg(q(x)) = 2$  and show how this leads to a contradiction.

- (b) Explain why  $\deg(q(x)) = 2$  implies that  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , and similarly that  $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ .
- (c) Part (b) gives us  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$ , and if so we would be able to write  $\sqrt{3} = a + b\sqrt{2}$  with  $a, b \in \mathbb{Q}$ . Square both sides and show how this would lead to a contradiction. (Do not forget to deal with the special cases  $a = 0$  or  $b = 0$ .)

Thus (after finishing (c)) we conclude that  $f(x)$  is the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ . Let us also try the other method of showing that  $f(x)$  is the minimal polynomial: showing that  $f(x)$  is irreducible over  $\mathbb{Q}$ .

- (d) Use one of the irreducibility tests from class to show that  $f(x)$  is irreducible over  $\mathbb{Q}$ . (There is more than one that will work.)

4. In this question we will explore some aspects of numbers algebraic over a fixed field.

- (a) Suppose that  $K \subseteq M$  is a field extension, with  $[M : K] = d$  (in particular, the degree of the extension is finite). Show that every  $\alpha \in M$  is algebraic over  $K$ , and satisfies a polynomial of degree  $\leq d$ . (SUGGESTION: Can  $1, \alpha, \dots, \alpha^d$  be linearly independent over  $K$ ?)
- (b) Let  $K \subseteq L$  be a field extension, and  $\alpha, \beta \in L$ . If  $\beta$  is algebraic over  $K$ , show that  $\beta$  is algebraic over  $K(\alpha)$ .
- (c) If  $\alpha, \beta \in L$  are both algebraic over  $K$ , show that  $[K(\alpha, \beta) : K]$  is finite.
- (d) If  $\alpha, \beta \in L$  are algebraic over  $K$  with  $\beta \neq 0$ , show that  $\alpha + \beta$ ,  $\alpha\beta$ , and  $\alpha/\beta$  are algebraic over  $K$ .
- (e) Consider the set  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ . Show that  $\overline{\mathbb{Q}}$  is a field.
- (f) Are there irreducible polynomials in  $\mathbb{Q}[x]$  of arbitrarily large degree?
- (g) Is  $[\overline{\mathbb{Q}} : \mathbb{Q}]$  finite or infinite?
- (h) Does the converse to (a) hold? I.e., if  $K \subseteq M$  is a field extension such that every  $\alpha \in M$  is algebraic over  $K$ , does this imply that  $[M : K]$  is finite?