

**Instructions:** Carefully write up solutions to the questions below. A solution should consist of both the answer and a careful explanation for why that answer must be correct. Any solutions without an explanation written out in English prose will receive no credit. You are welcome to work together, but write up solutions in your own, individual rules. Also, NO INTERNET!

(6pts) 1. Consider the field  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ , as well as the fields  $\mathbb{Q}(\sqrt{3})$  and  $\mathbb{Q}(\sqrt{5})$ .

- (a) Is  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$  an extension field of  $\mathbb{Q}(\sqrt{3})$ ? Is it an extension field of  $\mathbb{Q}(\sqrt{5})$ ? Explain. Hint: does  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$  contain  $\sqrt{15}$ ? If it does, then must also contain  $\sqrt{15}(\sqrt{3} + \sqrt{5}) - 3(\sqrt{3} + \sqrt{5})$ ?

**Solution:**  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$  contains  $(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$  so also contains  $\sqrt{15}$ . Then it must also contain  $\sqrt{15}(\sqrt{3} + \sqrt{5}) - 3(\sqrt{3} + \sqrt{5}) = 2\sqrt{3}$  so  $\sqrt{3}$ . Note that this also means that the field contains  $\sqrt{3} + \sqrt{5} - \sqrt{3} = \sqrt{5}$ .

All of this is to say that  $\sqrt{3}$  and  $\sqrt{5}$  are both already in  $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ , so this is an extension field of  $\mathbb{Q}(\sqrt{3})$  and also of  $\mathbb{Q}(\sqrt{5})$ .

- (b) If we take  $\mathbb{Q}(\sqrt{3})$  and adjoin  $\sqrt{5}$ , do we get a bigger field? We write  $\mathbb{Q}(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ . Draw a tower diagram showing how all the fields in this problem are related and explain why your diagram is accurate.

**Solution:** We do get a bigger field, since  $\sqrt{5}$  is not already in  $\mathbb{Q}(\sqrt{3})$  (if it were, we could write  $\sqrt{5} = a + b\sqrt{3}$ , but squaring both sides and rearranging would give  $\sqrt{3}$  as a rational number). The tower diagram will have  $\mathbb{Q}$  at the base, with  $\mathbb{Q}(\sqrt{3})$  and  $\mathbb{Q}(\sqrt{5})$  each above it (degree 2 extensions), each having  $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$  above them (also degree 2 extensions).

(4pts) 2. Find the minimum polynomials for:

- (a)  $\sqrt{3} + i$  over  $\mathbb{Q}(i)$

**Solution:**  $x^2 - 2ix - 4$  has  $\sqrt{3} + i$  as a root. Note that  $\sqrt{3} \notin \mathbb{Q}(i)$ ; if it were then  $\sqrt{3} = a + bi$  so  $3 = a^2 + 2abi - b^2$  and this says that  $i = \frac{3-a^2+b^2}{2ab}$  which is impossible ( $\sqrt{-1}$  is not a rational number). This proves that  $\sqrt{3} + i$  is not already in  $\mathbb{Q}(i)$  so the degree of the field extension  $\mathbb{Q}(\sqrt{3} + i)$  over  $\mathbb{Q}(i)$  is at least 2. Thus  $x^2 - 2ix - 4$  must be irreducible and the minimum polynomial we are looking for.

- (b)  $\sqrt{3} + i$  over  $\mathbb{Q}$ .

**Solution:** We have  $x^2 = 3 + 2\sqrt{3}i - 1$  so  $x^2 - 2 = 2\sqrt{3}i$ . Thus  $x^4 - 4x^2 + 4 = -12$  so we have that  $\sqrt{3} + i$  is a root of the polynomial  $x^4 - 4x^2 + 16$ . We can argue again that this must be the minimum polynomial because  $[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4$ .

(8pts) 3. Recall that we say an element  $a$  is *algebraic* over a field  $F$  if it is the root of a polynomial in  $F[x]$ .

- (a) Prove that  $a = \sqrt{3 + \sqrt[3]{5}}$  is algebraic over  $\mathbb{Q}$ .

**Solution:** All we need to do is find any polynomial that has  $a$  as a root. Start with  $x = \sqrt{3 + \sqrt[3]{5}}$  and square both sides. We get  $x^2 - 3 = \sqrt[3]{5}$ , so cube both sides to get  $x^6 - 9x^4 + 27x^2 - 27 = 5$  so  $a$  is a root of  $x^6 - 9x^4 + 27x^2 - 32$

- (b) Find a basis for  $\mathbb{Q}(a)$  over  $\mathbb{Q}(\sqrt[3]{5})$ . What is  $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt[3]{5})]$ ?

**Solution:** The degree is 2, as  $a$  is a root of  $x^2 - 3 - \sqrt[3]{5}$ . It takes some work to prove that the degree is not 1; to do so we would need to prove that  $a$  was not an element of  $\mathbb{Q}(\sqrt[3]{5})$  already. A basis for will be  $\{1, a\}$ .

- (c) Find a basis for  $\mathbb{Q}(a)$  over  $\mathbb{Q}$ . What is  $[\mathbb{Q}(a) : \mathbb{Q}]$ ?

**Solution:** Note that  $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ , so combining this with part (b) we have that  $[\mathbb{Q}(a) : \mathbb{Q}] = 6$ . A basis is  $\{1, a, a^2, a^3, a^4, a^5\}$  or alternatively  $\{1, \sqrt[3]{5}, \sqrt[3]{5}^2, a, a\sqrt[3]{5}, a\sqrt[3]{5}^2\}$

- (d) Find the *minimum* polynomial for  $a$  over  $\mathbb{Q}$  and prove it is irreducible (use part (c)).

**Solution:** In fact, since we know that the degree of  $\mathbb{Q}(a)$  over  $\mathbb{Q}$  is 6, the minimum polynomial for  $a$  will have degree 6. Further, any degree 6 polynomial which has  $a$  as a root will be irreducible (otherwise we would have  $a$  as a root of one of the factors which would have smaller degree. Thus the minimum polynomial is the one we found in (a):  $x^6 - 9x^4 + 27x^2 - 27$ .

- (6pts) 4. Which square roots are irrational? Let's find out.

- (a) Prove that if  $c$  is a root of an irreducible polynomial of degree greater than 1 in  $\mathbb{Q}[x]$ , then  $c$  is irrational. Your proof should use the math we have been doing recently.

**Solution:** We know that  $c \notin \mathbb{Q}$  because if it was the minimum polynomial for  $c$  would be  $x - c$ . But this has degree 1.

- (b) Let  $m, n \in \mathbb{Z}$  and consider  $\sqrt{m/n}$ . Suppose there is a prime  $p$  which divides  $m$  but not  $n$ , and that  $p^2$  does not divide  $m$ . Prove that  $\sqrt{m/n}$  is irrational. Hint: this should remind you of a particular criterion about polynomials.

**Solution:** Let's find a minimum polynomial for  $\sqrt{m/n}$ . Clearly  $x^2 - m/n$  has  $\sqrt{m/n}$  as a root. But is this irreducible? Well perhaps a better polynomial would be  $nx^2 - m$ . We can prove this is irreducible by Eisenstein's criterion!

- (6pts) 5. Prove that a regular 9-gon is not constructible (with a compass and straight-edge), but a regular 20-gon is. For the impossibility of the of the regular 9-gon, your proof should mimic the proof we did in class that  $20^\circ$  is not constructible. That is, your proof should talk about field extensions and polynomials (do not just argue that it is impossible because if we could construct it, we would then be able to construct  $20^\circ$  which we know is impossible).

**Solution:** To prove that a 9-gon is not constructible, we can simply show that  $40^\circ$  is not constructible (for if it were, we could easily construct a 9-gon using  $40^\circ$  as the central angle). Of course if  $40^\circ$  were constructible, then we could also construct  $20^\circ$ , which we proved in class was impossible. For a more direct proof, we use the triple angle formula for cosine:

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$$

Let  $\theta = 40^\circ$ , which gives  $-1/2 = \cos 120^\circ = 4\cos^3 40^\circ - 3\cos 40^\circ$ . This says that  $2\cos 40^\circ$  is a root of the polynomial  $x^3 - 3x + 1$ . But this polynomial is irreducible, which says that  $2\cos 40^\circ$  belongs to a degree 3 field extension of  $\mathbb{Q}$ . Since the constructible numbers only belong to field extensions of degrees powers of 2, it cannot be that  $\cos 40^\circ$  is constructible, so  $40^\circ$  is not constructible either.

A regular 20-gon is constructible if and only if  $18^\circ$  is constructible (the central angle), and this is constructible if and only if  $\cos 18^\circ$  is constructible. But  $\cos 18^\circ = \sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}$ , which is constructible since it is the result of combining integers using field operations and square roots.