

**M3P11 Galois Theory, Problem Sheet 2**

1. (a) Prove that if  $n \in \mathbb{Z}$  and  $\sqrt{n} \notin \mathbb{Z}$  then  $\sqrt{n} \notin \mathbb{Q}$ .  
 (b) Prove that  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ . What is the minimum polynomial of  $\sqrt{3}$  over  $\mathbb{Q}(\sqrt{2})$ ?  
 (c) Use the Tower Law to prove that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ .
2. (a) Prove that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Hint: the smallest subfield of the complex numbers containing  $\mathbb{Q}$  and  $\sqrt{2} + \sqrt{3}$  must contain loads of other things too: write some of them down.  
 (b) Deduce that  $x^4 - 10x^2 + 1$  is irreducible over  $\mathbb{Q}$ .
3. Is  $\sqrt{10} \in \mathbb{Q}(\sqrt{6}, \sqrt{15})$ ?
4. In this question, if  $\alpha \in \mathbb{R}_{>0}$  and  $n \in \mathbb{Z}_{\geq 1}$  then by  $\alpha^{1/n}$  or  $\sqrt[n]{\alpha}$  I mean the unique positive real number  $\beta$  with  $\beta^n = \alpha$ . (This removes ambiguities about a general complex number having  $n$  complex roots in this question).  
 (i) Set  $\gamma = (1 + \sqrt{3})^{1/3}$ . Prove that  $\gamma$  is algebraic. What is its degree over  $\mathbb{Q}$ ? What is its degree over  $\mathbb{Q}(\sqrt{3})$ ?  
 (ii) Set  $\delta = (10 + 6\sqrt{3})^{1/3}$ . Prove that  $\delta$  is algebraic. What is its degree over  $\mathbb{Q}$ ? What is its degree over  $\mathbb{Q}(\sqrt{2})$ ?
5. Prove that any subfield of  $\mathbb{C}$  must contain  $\mathbb{Q}$ .
6. Prove the part of the tower law that I didn't check: if  $E \subseteq K \subseteq F$  are fields, and one of  $[K : E]$  or  $[F : K]$  is infinite, then  $[F : E]$  is infinite.  
 Remark: for those unfamiliar with infinite-dimensional vector spaces, a vector space  $V$  over a field is infinite-dimensional iff it has no finite spanning set, iff for every  $n \geq 1$  there exist  $n$  elements  $v_1, v_2, \dots, v_n$  which are linearly independent.
7. Let  $A$  denote the set of complex numbers which are algebraic (over  $\mathbb{Q}$ ).  
 (i) Prove that  $A$  is a field.  
 (ii) Prove that  $[A : \mathbb{Q}] = \infty$ . Hint: you can use Eisenstein to construct irreducible polynomials of large degree...  
 (iii) Prove that  $A$  is a countable set.  
 (iv) Prove that  $[\mathbb{C} : A] = \infty$ .