THE UNIVERSITY OF SYDNEY

MATH3962: Rings, Fields and Galois Theory

(http://www.maths.usyd.edu.au/u/UG/SM/MATH3962/)

Semester 1, 2009 Lecturer: Adrian Nelson

Tutorial 8

1. A complex number α is called an *algebraic integer* if it is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$. (A polynomial is called *monic* if its leading coefficient is 1). Show that if $\alpha \in \mathbb{Q}$ is an algebraic integer then $\alpha \in \mathbb{Z}$. (Use the Rational Roots Theorem.)

2. Find a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ of which $\sqrt{3}+\sqrt{2}$ is a root. (Hint: make a guess as to three other real numbers which will also be roots of any such polynomial in $\mathbb{Q}[x]$.)

3. Let $\alpha \in \mathbb{C}$ be a root of $x^3+2x+2 \in \mathbb{Q}[x]$, and $\beta \in \mathbb{C}$ a root of $x^3-6x+3 \in \mathbb{Q}[x]$. Show that $\alpha+\beta$ is a root of a polynomial $f(x) \in \mathbb{Q}[x]$ of degree at most nine. (Hint: show that the elements $\alpha^i\beta^j$ with i, $j \in \{0,1,2\}$ span a finite dimensional $\mathbb{Q}$-subspace of $\mathbb{C}$ which is closed under multiplication, and in particular contains all the powers of $\alpha+\beta$.)

4. Let $\alpha = \sqrt[7]{2} \in \mathbb{R}$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α; that is, $f(x)$ is the least degree monic polynomial in $\mathbb{Q}[x]$ such that $f(\alpha) = 0$. Prove that $f(x)$ is a divisor of every $g(x) \in \mathbb{Q}[x]$ such that $g(\alpha) = 0$.

5. Let F be a field, E an extension field of F, and $t \in E$. Suppose that t is a root of some polynomial $f(x) \in F[x]$, and choose $f(x)$ to be such a polynomial with degree as small as possible. Prove that $f(x)$ is irreducible in $F[x]$. Is $f(x)$ irreducible as an element of $E[x]$?

6. Let F, E and t be as in Question 5. The *minimal polynomial* of t over F is the monic polynomial $f(x) \in F[x]$ of minimal degree with the property that $f(t) = 0$. Show that if $p(x) \in F[x]$ is irreducible and satisfies $p(t) = 0$ then $p(x)$ is an associate of the minimal polynomial of t. (That is, $p(x) = cf(x)$, where $c \in F$ and $f(x)$ is the minimal polynomial of t.)