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 9

1. (i) Let R be a principal ideal domain and I an ideal in R. Suppose that $\pi \in I$ is an irreducible element of R. Prove that if $I \neq R$, $I = \pi R$.

(ii) Let $\omega = e^{2\pi i/7} \in \mathbb{C}$, and let $\rho\colon \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation homomorphism determined by $x \mapsto \omega$. Find a polynomial $p(x) \in \mathbb{Q}[x]$ that generates the ideal $\ker\rho$. Hint: part (i) and a corollary of Eisenstein's Criterion from lectures will be relevant

2. 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 $f(\alpha) = 0$.

(i) Prove that $f(x)$ is a divisor of every $g(x) \in \mathbb{Q}[x]$ such that $g(\alpha) = 0$. (Hint: $g(x) = q(x)f(x)+r(x)$ for some polynomial $r(x)$ of degree less than $\deg f(x)$.)

(ii) Use Eisenstein's Criterion to prove that $x^7 - 2 \in \mathbb{Q}[x]$ is irreducible.

(iii) Deduce that $f(x) = x^7 - 2$.

(iv) Considering $\mathbb{R}$ as a vector space over $\mathbb{Q}$, prove that the seven elements α^i with $0 \leq i \leq 6$ are linearly independent.

(v) Prove that the seven dimensional $\mathbb{Q}$-subspace E of $\mathbb{R}$ spanned by the powers of α is in fact a subfield of $\mathbb{R}$.

(vi) Express the inverse of $\alpha^2 + 1$ as a $\mathbb{Q}$-linear combination of powers of α.

3. Noting that $x^2 + 1 \in \mathbb{R}[x]$ is irreducible and that $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[-i]$ where i and $-i$ are complex roots of $x^2 + 1$, show that there are two different isomorphisms $\mathbb{R}[x]/K \to \mathbb{C}$, where $K = (x^2 + 1)\mathbb{R}[x]$, one satisfying $f(x) + K \mapsto f(i)$, the other $f(x) + K \mapsto f(-i)$, for all $f(x) \in \mathbb{R}[x]$.

4. Let n be a positive integer and $C_n = \{1, g, g^2, \ldots, g^{n-1}\}$ the cyclic group of order n. Show that for each positive divisor d of n the set of powers of g^d form a cyclic group of order n/d. Show furthermore that if $\gcd(r, n) = d$ then the set of powers of g^r coincides with the set of powers of g^d.

5. Suppose that a, b, $c \in \mathbb{C}$ are the roots of $x^3 + 9x^2 + 3x - 3 \in \mathbb{Z}[x]$. By expressing the numbers $a^2 + b^2 + c^2$, $a^2b^2 + a^2c^2 + b^2c^2$ and $a^2b^2c^2$ in terms of $a + b + c$, $ab + ac + bc$ and abc, find a polynomial $f(x) \in \mathbb{Z}[x]$ whose roots are a^2, b^2 and c^2.