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 6

1. (*i*) Use the Euclidean Algorithm to show that $\gcd(23, 14) = 1$ and find integers r, s such that $14r + 23s = 1$. Hence find the inverse of 14 in $\mathbb{Z}_{23}$.

(*ii*) Let $I = (x^3 - 2)\mathbb{Q}[x]$, an ideal in $\mathbb{Q}[x]$. Use the Euclidean Algorithm in $\mathbb{Q}[x]$ to find a polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(x)+I$ is the inverse of $(x^2-x+2)+I$ in $\mathbb{Q}[x]/I$. Hence express $\frac{1}{(\sqrt[3]{2})^2-\sqrt[3]{2}+2}$ in the form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$, with a, b, $c \in \mathbb{Q}$.

2. Find the unique monic polynomial $d(x) \in Z_2[x]$ that is a greatest common divisor of $r(x) = x^4 + x^3 + x^2 + 1$ and $s(x) = x^3 + 1$. Find polynomials $a(x)$ and $b(x)$ in $\mathbb{Z}_2[x]$ such that $d(x) = a(x)r(x) + b(x)s(x)$.

3. (*i*) Find all irreducible quadratics, cubics and quartics in $\mathbb{F}_2[x]$.

(*ii*) Find all irreducible monic quadratic and cubics in $\mathbb{F}_3[x]$.

4. Let R be a principal ideal domain. Show direct from the definitions that a non-zero $\pi \in R$ is irreducible if and only if πR is a maximal ideal.

5. Let $\mathbb{G} = \{\, n + mi \mid n,\ m \in \mathbb{Z} \,\} \subseteq \mathbb{C}$, the ring of *Gaussian integers*.

(*i*) List all the elements of the quotient ring $S = \mathbb{G}/3\mathbb{G}$, and write out complete addition and multiplication tables for S.

(*ii*) Use your multiplication table to show that every nonzero element of S has a multiplicative inverse, and deduce that S is a field.