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 5

1. Let R be a principal ideal domain and $p \in R$ an irreducible element. Prove that R/pR is a field as follows. Show that if $a \in R$ is such that $p \nmid a$ then p and a have greatest common divisor 1. So there exist $r, s \in R$ with $ra + sp = 1$. Deduce that element $a + pR$ of the quotient ring R/pR has an inverse (namely, $r + pR$). Deduce that every non-zero element of R/pR has an inverse.

2. An ideal I in a ring R is said to be *prime* if $I \neq R$ and the following condition is satisfied:

$$\text{for all } a, b \in R, \text{ if } ab \in I \text{ then } a \in I \text{ or } b \in I.$$

Let R be a commutative ring with 1 and I an ideal in R. Prove that I is prime if and only if R/I is an integral domain.

3. (Third Isomorphism Theorem) Let I and J be ideals in the ring R with $I \subseteq J$. Show that $a+I \mapsto a+J$ for all $a \in R$ defines a surjective homomorphism $R/I \to R/J$. Use the First Isomorphism Theorem to deduce that J/I is an ideal in R/I and $(R/I)\big/(J/I) \cong R/J$.

Now conversely suppose that K is an ideal of R/I. Show that the kernel of of the composite of the canonical map from R to R/I and the canonical map from R/I to $(R/I)/K$, $J = \{x \in R : x + I \in K\}$ is an ideal of R containing I such that $K = J/I$.

4. An ideal I in a ring R is said to be *maximal* if $I \neq R$ and the only ideals J in R such that $I \subseteq J$ are I and R.

Suppose that R is a commutative ring with 1 and that I is a maximal ideal in R. Show that if $a, b \in R$ are arbitrary elements such that $a \notin I$ then there exists $x \in R$ such that $b + I = ax + I$. (Hint: consider the ideal $I + aR$.) Deduce that R/I is a field.

5. Let R be a principal ideal domain. Show that a non-zero $p \in R$ is irreducible if and only if pR is a maximal ideal.

6. How many distinct functions are there from the two-element field $\mathbb{F}_2$ to itself? How many of these are polynomial functions? And how many elements are there in $\mathbb{F}_2[x]$, the set of all polynomials over $\mathbb{F}_2$ in the indeterminate x?