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 2

1. Let G be a group and S a set on which a multiplication operation is defined. Let $\phi\colon G \to S$ be a function that satisfies $(\phi x)(\phi y) = \phi(xy)$ for all x, $y \in G$. Prove that the image of ϕ is a group, with multiplication compatible with multiplication in S.

2. Let S be a set with a multiplication operation. An element $e \in S$ is called a *left identity* if $es = s$ for all $s \in S$, and an element $f \in S$ is called a *right identity* if $sf = s$ for all $s \in S$.

(i) Prove that if S contains both a left identity and a right identity then they are equal.

(ii) Find an example of an S that contains a left identity but no right identity. (Hint: use 2×2 matrices.)

3. Let R be a ring and define $R^n = \{\, (x_1, x_2, \ldots, x_n) \mid x_i \in R \,\}$, where n is a fixed positive integer. Define addition and multiplication on R^n by the rules

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$
$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

Is it true, for all R and n, that R^n is a ring under these operations?

4. Let R be a ring with the property that $a^2 = a$ for all $a \in R$. Prove that $a + a = 0$ for all $a \in R$, and that R is commutative. Show also that R, with its given addition operation, can be made into a vector space over the field of two elements.

5. If X is any set and R any ring then the set of all functions from X to R becomes a ring if addition and multiplication of functions is defined "pointwise". That is, fg and $f + g$ are given by $(fg)(x) = (f(x))(g(x))$ and $(f + g)(x) = f(x) + g(x)$. Take R to be the two-element field $\mathbb{F}_2 = \{0, 1\}$, and for each $A \subseteq X$ define $f_A\colon X \to \mathbb{F}_2$ by the rule that $f_A(x)$ is 1 if $x \in A$ and 0 if $x \notin A$. Show that $f_A f_B = f_{A\cap B}$ and $f_A + f_B = f_{A\Delta B}$ for all A, $B \subseteq X$, where Δ is the "symmetric difference" operation: $A \,\Delta\, B$ consists of the elements of A that are not in B and the elements of B that are not in A.

6. Which of the following are rings?

(i) The set $\mathbb{R}^3$, with addition defined in the usual way, and multiplication given by $(a, b, c) \times (d, e, f) = (bf - ce, cd - af, ae - bd)$.

(ii) The set of all rational numbers expressible in the form a/b, where a and b are integers and p does not divide b. Here p denotes a fixed prime integer, and the operations are the usual ones.

(iii) The set of integers with a new addition $\oplus$ and a new multiplication $\otimes$ defined in terms of the usual operations by

$$n \oplus m = n + m + 1,$$
$$n \otimes m = n + m + nm.$$

7. Let C be a cyclic group of order n (so that $C = \{1, x, \ldots, x^{n-1}\}$ and $x^n = 1$.) The *group algebra* $\mathbb{R}C$ consists of all formal linear combinations $\sum_{i=0}^{n-1} \lambda_i x^i$, with $\lambda_i \in \mathbb{R}$, with addition, multiplication and scalar multiplication defined so that all the ring and vector space axioms are satisfied. Show that $\mathbb{R}C$ is not an integral domain.