Math 516 **Fall 2008** **Radford**

Written Homework # 5 Solution

12/03/08

---

1. (**20 points**) Note that if $R_1, \ldots, R_n$ are finite Boolean rings then the direct product $R_1 \times \cdots \times R_n$ is a Boolean ring also. Thus part (c) characterizes finite Boolean rings.

(a) (**8 pts**) Let $a, b \in R$. The calculation $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$ shows that $0 = ab + ba$. Therefore $ab = -ba$. With $b = 1$ we have $a = -a$ which means $\boxed{x = -x \text{ for all } x \in R}$. Thus $ab = -ba = ba$.

(b) (**6 pts**) Since R is commutative by part (a) the left ideals Re and $R(1 - e)$ of R are ideals. Let $a \in R$. Then $1 = e + (1 - e)$ means $a = ae + a(1 - e) \in Re + R(1 - e)$. Therefore $R = Re + R(1 - e)$.

Suppose that $a \in Re \cap R(1 - e)$. Then $a = xe = y(1 - e)$ for some $x, y \in R$. But then $a = xe = xe^2 = y(1 - e)e = y(e^2 - e) = y(e - e) = 0$. We have shown that $Re \cap R(1 - e) = (0)$.

(c) (**6 pts**) For $a \in R$ note that the (left) ideal Ra is a Boolean ring with identity element a (as $a(ra) = (ra)a = ra^2 = ra$). If $|R| = 2$ then $R \simeq \mathbf{Z}_2$ by part (a). Suppose that $|R| > 2$. Then there an $e \in R$ with $e \neq 0, 1$. Therefore $Re, R(1-e) \neq (0)$ and are thus proper subsets of R by part (b). By induction on $|R|$ we have $Re \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$ (m factors) and $R(1 - e) \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$ (n factors) for some $m, n \geq 1$. Therefore

$$R = Re \oplus R(1 - e) \simeq (\mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2) \times (\mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2) \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2.$$

Comment: You should show that the maps above are isomorphisms of rings.

2. (**20 points**) The point of this problem is that lack of identity element in a ring is not a fundamental problem and that the rings $\mathrm{End}(A)$, where A is an abelian group, are to general rings as permutation groups are to general groups.

(a) (**12 pts**) What is to be shown is that R with the given multiplication is a monoid and the distributive laws hold. The laws for multiples (the additive analogs of the exponent laws for abelian groups) are used.

(b) (**8 pts**) For $r \in R$ define $\ell_r : R \longrightarrow R$ by $\ell_r(r') = rr'$ for all $r' \in R$. Since $\ell_r(r' + r'') = r(r' + r'') = rr' + rr'' = \ell_r(r') + \ell_r(r'')$ for all $r', r'' \in R$ we have that $\ell_r \in \mathrm{End}(R)$, where R is regarded as an abelian group.

Define $\pi : R \longrightarrow \mathrm{End}(R)$ by $\pi(r) = \ell_r$. The equations

$$\ell_{r+r'}(r'') = (r + r')r'' = rr'' + r'r'' = \ell_r(r'') + \ell_{r'}(r'')$$

for all $r, r', r'' \in R$ show that $\ell_{r+r'} = \ell_r + \ell_{r'}$ for all $r, r' \in R$ and the equations

$$\ell_{rr'}(r'') = (rr')r'' = r(r'r'') = \ell_r(\ell_{r'}(r'')) = (\ell_r \circ \ell_{r'})(r'')$$

for all $r, r', r'' \in R$ show that $\ell_{rr'} = \ell_r \circ \ell_{r'}$ for all $r, r' \in R$. Therefore π is a ring homomorphism.

Suppose that R has unity 1 and $r \in \mathrm{Ker}\,\pi$. Then $\pi(r) = 0$; in particular $0 = \pi(r)(1) = r1 = r$. Therefore $\mathrm{Ker}\pi = (0)$ which means that π is injective. Thus take $A = \mathbf{R}$ and $\jmath : R \longrightarrow \mathrm{End}(A)$ to be the composite of injective ring homomorphisms $R \xrightarrow{\imath} \mathbf{R} \xrightarrow{\pi} \mathrm{End}(A)$.

3. (**20 points**) Since $\mathbf{Z}_2$ is a field $\mathbf{Z}_2[x]$ is a unique factorization domain. Suppose $f(x) \in \mathbf{Z}_2[x]$. If $f(x)$ has degree 2 or 3 then $f(x)$ is *reducible* if and only if has a root (equivalently has a linear factor).

Suppose that $f(x)$ has degree 4. Then $f(x)$ is reducible if and only if it has a root (equivalently has a linear factor) or is the product of two irreducible quadratic factors.

Case 1: $\deg f(x) = 2$. Then $f(x) = x^2 + ax + b$. Since $f(0) = b$ and $f(1) = 1 + a + b$, $f(x)$ is reducible if and only if $b = 0$ or $1 + a + b = 0$. Thus $f(x)$ is *irreducible* if and only if $b \neq 0$ and $1 + a + b \neq 0$; that is $b = 1$ and $1 + a + b = 1$ or equivalently $b = 1 = a$. $\boxed{x^2 + x + 1.}$

Comment: Here is another way. $f(x)$ is reducible if and only if $f(x) = (x - \alpha)(x - \beta)$, where $\alpha, \beta \in \mathbf{Z}_2$. There are three such polynomials out of the four degree 2 polynomials. Thus there is one irreducible polynomial of degree 2. Since $x^2 + x + 1$ has no roots in $\mathbf{Z}_2$, this is the irreducible one.

Case 2: $\deg f(x) = 3$. Then $f(x) = x^3 + ax^2 + bx + c$. Since $f(0) = c$ and $f(1) = 1 + a + b + c$, $f(x)$ is reducible if and only if $c = 0$ or $1 + a + b + c = 0$. Therefore $f(x)$ is irreducible if and only if $c = 1$ and $1 + a + b + c = 1$ or equivalently $c = 1$ and $a + b + 1 = 0$. Thus $\boxed{x^3 + x^2 + 1, x^3 + x + 1.}$

Case 3: $\deg f(x) = 4$. Then $f(x) = x^4 + ax^3 + bx^2 + cx + d$. Since $f(0) = d$ and $f(1) = 1 + a + b + c + d$ it follows that $f(x)$ is reducible if and only if $d = 0$, or $1 + a + b + c + d = 0$, or $f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1$. Thus $f(x)$ is irreducible if and only if $d = 1$ and $a + b + c + 1 = 0$ and $f(x) \neq x^4 + x^2 + 1$. $\boxed{x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1.}$

4. (**20 points**) Recall that $\prod_{i \in I} M_i$ is a group by WH2 Exercise 1.

(a) (**8 pts.**) We have noted that $\prod_{i\in I} M_i$ is a group. It is abelian since each M_i is abelian and by definition of the addition in $\prod_{i\in I} M_i$.

Suppose $r, r' \in R$ and $f, f' \in \prod_{i\in I} M_i$. The calculation

$$\begin{aligned}(r\cdot(f+f'))(\imath) &= r\cdot((f+f')(\imath)) \\ &= r\cdot(f(\imath)+f'(\imath)) \\ &= r\cdot(f(\imath))+r\cdot(f'(\imath)) \\ &= (r\cdot f)(\imath)+(r\cdot f')(\imath) \\ &= (r\cdot f+r\cdot f')(\imath)\end{aligned}$$

for all $\imath \in I$ shows that $r\cdot(f+f') = r\cdot f + r\cdot f'$. Likewise the calculation

$$\begin{aligned}((r+r')\cdot f)(\imath) &= (r+r')\cdot(f(\imath)) \\ &= r\cdot(f(\imath))+r'\cdot(f(\imath)) \\ &= (r\cdot f)(\imath)+(r'\cdot f)(\imath) \\ &= (r\cdot f+r'\cdot f)(\imath)\end{aligned}$$

for all $\imath \in I$ shows that $(r+r')\cdot f = r\cdot f + r'\cdot f$. Finally, the calculation

$$((rr')\cdot f)(\imath) = (rr')\cdot(f(\imath)) = r\cdot(r'\cdot f(\imath)) = r\cdot((r'\cdot f)(\imath)) = (r\cdot(r'\cdot f))(\imath)$$

for all $\imath \in I$ shows that $(rr')\cdot f = r\cdot(r'\cdot f)$.

(b) (**12 pts.**) Suppose that M is a left R-module and $\pi_i' : M \longrightarrow M_i$ is a homomorphism of left R-modules for all $i \in I$. Further assume that $F : M \longrightarrow \prod_{i\in I} M_i$ is a homomorphism of left R-modules which satisfies $\pi_i \circ F = \pi_i'$ for all $i \in I$. Then for $m \in M$ the calculation

$$F(m)(i) = \pi_i(F(m)) = (\pi_i \circ F)(m) = \pi_i'(m)$$

shows that $F(m)(i) = \pi_i'(m)$ for all $i \in I$. This last equation determines F.

Conversely, suppose that $F : M \longrightarrow \prod_{i\in I} M_i$ is a function which satisfies the last equation. Then $\pi_i \circ F = \pi_i'$ for all $i \in I$ as

$$(\pi_i \circ F)(m) = \pi_i(F(m)) = F(m)(i) = \pi_i'(m)$$

for all $i \in I$ and $m \in M$. Let $m, m' \in M$. Observe that

$$F(m+m')(i) = \pi_i(m+m') = \pi_i(m)+\pi_i(m') = F(m)(i)+F(m')(i) = (F(m)+F(m'))(i)$$

for all $i \in I$ which means that $F(m+m') = F(m) + F(m')$. Since

$$F(r\cdot m)(i) = \pi_i'(r\cdot m) = r\cdot(\pi_i'(m)) = r\cdot(F(m)(i)) = ((r\cdot F)(m))(i)$$

for all $r \in R$, $m \in M$, and $i \in I$ we have $F(r \cdot m) = r \cdot F(m)$ for all $r \in R$ and $m \in M$.

5. (**20 points**) We sketch a proof. We continue with the ideas of WH4 Exercise 1. For $f \in \prod_{i \in I} M_i$ set $S_f = \{i \in I \mid f(i) \neq 0\}$. Then

$$S_{f+g} \subseteq S_f \cup S_g, \quad S_{-f} = S_f, \quad \text{and} \quad S_{r \cdot f} \subseteq S_f \tag{1}$$

for all $f, g \in \prod_{i \in I} M_i$ and $r \in R$. The last inclusion follows by $i \notin S_{r \cdot f}$ implies $i \notin S_f$.

Let

$$M = \{f \in \prod_{i \in I} M_i \mid S_f \text{ is finite}\}$$

Observe that $S_{\mathbf{0}} = \emptyset$, where $\mathbf{0} \in \prod_{i \in I} M_i$ defined by $\mathbf{0}(i) = 0$ for all $i \in I$. Thus $\mathbf{0} \in M$. Thus M is a submodule of $\prod_{i \in I} M_i$ by virtue of (1).

Let $i \in I$. Note that $\jmath_i$ is a module map. Since $S_{\jmath_\imath(m)}$ has at most one element for all $m \in M_\imath$ it follows that $\operatorname{Im} \jmath_\imath \subseteq M$. Therefore we may regard $\jmath_\imath$ as a module map $\jmath_\imath : M_\imath \longrightarrow M$.

Suppose $f \in M$. Then

$$f = \sum_{i \in S_f} \jmath_i(f(i)) \tag{2}$$

as both sides agree on all $\ell \in I$. If $S_f = \emptyset$, that is $f = \mathbf{0}$, by convention the sum on the right hand side is $\mathbf{0}$.

Now suppose that N is a left R-module and $\{\jmath'_i\}_{i \in I}$ is a family of left R-module maps, where $\jmath'_i : M_i \longrightarrow N$ for all $i \in I$. Suppose that $F : M \longrightarrow N$ is a left R-module map which satisfies $F \circ \jmath_i = \jmath'_i$ for all $i \in I$. Using (2) we see

$$F(f) = F(\sum_{i \in S_f} \jmath_i(f(i))) = \sum_{i \in S_f} F(\jmath_i(f(i))) = \sum_{i \in S_f} F \circ \jmath_i(f(i)) = \sum_{i \in S_f} \jmath'_i(f(i))$$

and therefore

$$F(f) = \sum_{i \in S_f} \jmath'_i(f(i)). \tag{3}$$

In particular there is at most one map of left R-modules $F' : M \longrightarrow N$ such that $F' \circ \jmath_i = \jmath'_i$ for all $i \in I$.

Let $F : M \longrightarrow N$ be the function defined by (3). Note that if T is a finite subset of I and $S_f \subseteq T$ then $F(f) = \sum_{i \in T} \jmath'_i(f(i))$ since $i \in T \backslash S_f$ means that $f(i) = 0$. It is a straightforward check that F is a map of left R-modules which satisfies $F \circ \jmath_i = \jmath'_i$ for all $i \in I$. See the solution to WH4 Exercise 1.