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

Written Homework # 4 Solution

12/02/08

1. (**20 points**) For $f \in \mathcal{G} = \mathrm{Fun}(S, G)$ set $S_f = \{s \in S \,|\, f(s) \neq 0\}$. This set is sometimes called the support of f. Let $g \in \mathcal{G}$ also. Observe that

$$S_f = S_{-f} \tag{1}$$

and

$$S_{f+g} \subseteq S_f \cup S_g. \tag{2}$$

To see that latter observe that $s \notin S_f \cup S_g$ implies $s \notin S_{f+g}$ which is an equivalent statement.

(a) (**6 pts**) Note the function $\mathbf{0} : S \longrightarrow G$ defined by $\mathbf{0}(s) = 0$ for all $s \in S$ belongs to $\mathcal{G}$ since $S_{\mathbf{0}} = \emptyset$. Thus $\mathrm{A}(S, G) \neq \emptyset$.

Let $f, g \in \mathrm{A}(S, G)$. Then S_f, S_g are finite. Since $S_{f-g} = S_{f+(-g)} \subseteq S_f \cup S_{-g} = S_f \cup S_g$ by (1) and (2), it follows that S_{f-g} is finite as the union of finite sets is finite. Therefore $f - g \in \mathrm{A}(S, G)$ and we have established $\mathrm{A}(S, G) \leq \mathcal{G}$.

(b) (**14 pts**) Suppose that $f \in \mathrm{A}(S, \mathrm{Z})$, $T \subseteq S$ is finite, and $S_f \subseteq T$. Then

$$\left(\sum_{t \in T} f(t)\imath(t)\right)(s) = \sum_{t \in T} f(t)\imath(t)(s) = \left\{ \begin{array}{ccl} 0 & : & s \notin T \\ 0 & : & s \in T \text{ and } s \notin S_f \\ f(s) & : & s \in T \text{ and } s \in S_f \end{array} \right.$$

Therefore

$$f = \sum_{t \in T} f(t)\imath(t) \tag{3}$$

Note that $\mathrm{A}(S, \mathbf{Z})$ is abelian since $\mathbf{Z}$ is. To show that $(\imath, \mathrm{A}(S, \mathbf{Z}))$ is a free abelian group on S we need to establish the following: Suppose that $(\jmath, G)$ ia a pair, where $\jmath : S \longrightarrow G$ is a set map and G is an abelian group, there is a group homomorphism $F : \mathrm{A}(S, \mathbf{Z}) \longrightarrow G$ determined by $F \circ \imath = \jmath$.

Suppose that that $F : \mathrm{A}(S, \mathbf{Z}) \longrightarrow G$ is *any* group homomorphism satisfying $F \circ \imath = \jmath$. Let $f \in \mathrm{A}(S, \mathbf{Z})$. Then by (3)

$$\begin{aligned} F(f) &= F(\sum_{s \in S_f} f(s)\imath(s)) \\ &= \sum_{s \in S_f} F(f(s)\imath(s)) \\ &= \sum_{s \in S_f} f(s)F(\imath(s)) \\ &= \sum_{s \in S_f} f(s)((F \circ \imath)(s)) \\ &= \sum_{s \in S_f} f(s)(\jmath(s)). \end{aligned}$$

We have established uniqueness.

Existence. Define F by $F(f) = \sum_{s \in S_f} f(s)\jmath(s)$ for $f \in \mathrm{A}(S, \mathbf{Z})$. Then

$$(F \circ \imath)(s) = F(\imath(s)) = \sum_{s' \in S_{\imath(s)}} \imath(s)(s')(\jmath(s')) = \imath(s)(s)(\jmath(s)) = 1(\jmath(s)) = \jmath(s)$$

which shows that $F \circ \imath = \jmath$. Observe that if $T \subseteq S$ is finite and $S_f \subseteq T$ then

$$\sum_{s \in S_f} f(s)\jmath(s) = \sum_{t \in T} f(t)\jmath(t) \tag{4}$$

since $f(t) = 0$ for all $t \in T \backslash S_f$. Thus for $f, g \in \mathrm{A}(S, \mathbf{Z})$ we have by (4)

$$\begin{aligned} F(f+g) &= \sum_{s \in S_{f+g}} (f+g)(s)\jmath(s) \\ &= \sum_{s \in S_f \cup S_g} (f+g)(s)\jmath(s) \\ &= \sum_{s \in S_f \cup S_g} (f(s)+g(s))\jmath(s) \\ &= \sum_{s \in S_f \cup S_g} f(s)\jmath(s) + \sum_{s \in S_f \cup S_g} g(s)\jmath(s) \\ &= F(f) + F(g) \end{aligned}$$

which completes our proof.

2. (**20 points**) Here we pick up on a fundamental argument for cyclic groups.

(a) (**8 pts**) Since the set $\{1, a, a^2, \ldots\}$ is finite there are integers $0 \leq \ell < n$ such that $a^\ell = a^n$. We can assume that n is the smallest such integer.

Suppose that $\ell = 0$. Then $n - 1 \geq 0$ and $aa^{n-1} = a^{n-1}a = a^n = a^0 = 1$. Therefore a has a multiplicative inverse which is a^{n-1}.

Suppose $\ell > 0$. Then $m - 1 > \ell - 1 \geq 0$ and

$$a(a^{n-1} - a^{\ell-1}) = (a^{n-1} - a^{\ell-1})a = a^n - a^\ell = 0.$$

By the minimality of n we have $b = a^{n-1} - a^{\ell-1} \neq 0$. Now $0 = ab = ba$.

(b) (**5 pts**) Follows immediately by part (a).

(c) (**7 pts**) Since R is a finite-dimensional vector space over F the set $\{1, a, a^2, \ldots\}$ is dependent. Now $\{1\} = \{a^0\}$ is independent. Therefore there is an $n \geq 1$ so that $\{1, \ldots, a^{n-1}\}$ is independent and $\{1, \ldots, a^n\}$ is independent. There is a dependency relation

$$\alpha_0 1 + \cdots + \alpha_n a^n = 0$$

where $\alpha_n \neq 0$. Multiplying both sides of this equation by α_0^{-1} we may assume $\alpha_n = 1$. Observe that

$$a(\alpha_1 1 + \cdots + a^{n-1}) = (\alpha_1 1 + \cdots + a^{n-1})a = \alpha_1 a + \cdots + a^n = -\alpha_0 1.$$

Suppose that $\alpha_0 \neq 0$. Then a has a multiplicative inverse which is $a^{-1} = -\alpha_0^{-1}(\alpha_1 1 + \cdots + a^{n-1})$.

Suppose that $\alpha_0 = 0$. Then $ab = ba = 0$, where $b = \alpha_1 1 + \cdots + a^{n-1}$. By the minimality of n we see that $b \neq 0$.

3. (**20 points**) We are assuming the binomial theorem for commutative rings.

(a) (**5 pts**) Suppose that $a \in R$ is nilpotent. Then $a^m = 0$ for some positive integer m. Let $\ell \geq m$. Then $\ell - m \geq 0$ and $a^\ell = a^m a^{m-\ell} = 0a^{m-\ell} = 0$. Since $(-a)^n = \begin{cases} a^n & : n \text{ even} \\ -a^n & : n \text{ odd} \end{cases}$ it follows that $(-a)^m = 0$ as well.

Suppose that $b \in R$ is also nilpotent. To show that $a \pm b$ is nilpotent we need only show that $a + b$ is nilpotent by our comments above. Now $b^n = 0$ for some positive integer n. Now $m + n - 1$ is a positive integer and

$$(a+b)^{m+n-1} = \sum_{\ell=0}^{m+n-1} \binom{m+n-1}{\ell} a^{m+n-1-\ell} b^\ell.$$

Let $0 \leq \ell \leq m + n - 1$. If $m + n - 1 - \ell < m$ and $\ell < n$ then

$$m + n - 1 = (m + n - 1 - \ell) + \ell \leq (m - 1) + (n - 1) = m + n - 2 < m + n - 1,$$

a contradiction. Therefore $m + n - 1 - \ell \geq m$, in which case $a^{m+n-1-\ell} = 0$, or $\ell \geq n$, in which case $b^\ell = 0$. Thus $a^{m+n-1-\ell} b^\ell = 0$. We have shown that $(a + b)^{m+n-1} = 0$. Therefore $a + b$ is nilpotent.

(b) (**5 pts**) Since $ar = ra$, it follows that $(ar)^n = a^n r^n$ for all positive integers n. Thus $a^m = 0$ implies $(ar)^m = 0r^m = 0$.

(c) (**5 pts**) Note $0 \in N$ as $0^1 = 0$. Thus N is an additive subgroup of R by part (a) and consequently N is an ideal of R by part (b).

(d) (**5 pts**) Let $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $a + b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Since $(a+b)^2 = \mathrm{I}_2$ it follows that $(a+b)^{2n} = \mathrm{I}_2$. Therefore $a+b$ is not nilpotent as $(a+b)^n = 0$ implies $(a+b)^{2n} = 0$.

Now $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ satisfies $(ab)^2 = ab \neq 0$. Thus $(ab)^n = ab$ for all $n \geq 1$, by induction on n, which means that ab is not nilpotent.

4. (**20 points**) Let $0 \neq f(x) \in F((x))$. Then $f(x) = \sum_{n=N}^{\infty} a_n x^n$ for some $N \in \mathbf{Z}$ where $a_N \neq 0$.

(a) (**10 pts**) We define a sequence $b_{-N}, b_{-N+1}, b_{-N+2}, \ldots$ by $b_{-N} = a_N^{-1}$ and

$$b_{-N+n} = -a_N^{-1} \left(\sum_{\ell=1}^{n} a_{N+\ell} b_{-N+n-\ell} \right)$$

for $n > 0$. Then $a_N b_{-N} = 1$ and

$$\sum_{\ell=0}^{n} a_{N+\ell} b_{-N+n-\ell} = 0$$

for $n > 0$. Set $g(x) = \sum_{n=-N}^{\infty} b_n x^n$. As $a_i b_j = 0$ unless $i \geq N$ and $j \geq -N$, we have

$$f(x)g(x) = \sum_{n} \left(\sum_{i+j=n} a_i b_j \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{\ell=0}^{n} a_{N+\ell} b_{-N+n-\ell} \right) x^n = 1 + 0x + 0x^2 + \cdots = 1.$$

Since $F((x))$ is commutative $f(x)$ and $g(x)$ are inverses.

(b) (**10 pts**) Now suppose $f(x) \in F[[x]]$. Then $N \geq 0$. Since $b_{-N} \neq 0$, $g(x) \in F[[x]]$ if and only if $-N \geq 0$ as well; thus if and only if $N \geq 0 \geq N$ or equivalently $N = 0$. The latter is the case if and only if $a_0 \neq 0$.

5. (**20 points**) Let n be a positive integer and suppose that R is commutative ring with unity such that $a^n = a$ for all $a \in R$. First of all we show that if R is an integral domain then R is a field.

Suppose R is an integral domain. Let $0 \neq a \in R$. Then $n - 1 \geq 0$ and $a(a^{n-1}) = a^n = a = 1a$. Thus $a^{n-1} = 1$ by cancellation. If $n = 1$ then $a = 1$; otherwise $n-2 \geq 0$ and $aa^{n-2} = 1 = a^{n-2}a$. In any case a has a multiplicative inverse. We have shown that R is a field.

Now suppose P is a prime ideal of R. Then R/P is an integral domain and the hypothesis for R holds for R/P. Therefore R/P is a field which means that P is a maximal ideal of R.