Shashank Singh
sss1@andrew.cmu.edu

21-373 Honors Algebraic Structures, Fall 2011
Assignment 4
Due: Friday, October 7

The following lemmas are referenced in the below proofs:

Lemma 1: Suppose R is a ring with $x, y \in R$. Then, (1) $0x = 0 = x0$, (2) $(-x)y = -(xy) = x(-y)$, and (3) $(-x)^2 = x^2$.

Proof: By definition of additive identity and by distributivity, $0x = (0+0)x = 0x + 0x$. Adding $0x$ gives $0 = 0x$. Similarly, $x0 = x(0+0) = x0 + x0$, so $x0 = 0$, proving (1). Furthermore, $ab + -(ab) = 0 = 0b = (a + (-a))b = ab + (-a)b$, so since the additive identity on of a ring is unique (as the ring is a group under addition), $-(ab) = (-a)b$. Similarly, $ab + -(ab) = 0 = a0 = a(b + (-b)) = ab + a(-b)$, so $-(ab) = a(-b)$ proving (2). As a consequence, $(-x)^2 = -(x(-x)) = -(-(xx)) = xx = x^2$, showing (3). ■

Lemma 2: Suppose R is a commutative ring, with $a, b \in R$. Then, $\forall n \in \mathbb{N}$, $(ab)^n = a^n b^n$.

Proof: Let $a, b \in R$. For $n = 1$, clearly $(ab)^n = ab = a^n b^n$. Suppose that, for some $n \in \mathbb{N}$, $(ab)^n = a^n b^n$. Then, since R is commutative and associative, $(ab)^{n+1} = (ab)^n(ab) = (a^n b^n)(ab) = (a^n a)(b^n b) = a^{n+1}b^{n+1}$, so, by the Principle of Mathematical Induction the lemma is proven.

Lemma 3: Let R be a commutative ring, and let $a, b \in R$. Then, $\forall n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} c_n a^k b^{n-k}$$

for some constants $c_0, c_1, \dots, c_n \in \mathbb{N}$. Note that this lemma is essentially a weakened form of the Binomial theorem generalized to commutative rings (the stronger form is not shown because its algebraic proof requires use of Pascal's identity, which is beyond the current scope).

Proof: Suppose R is a commutative ring, and let $a, b \in R$. Then, for $n = 1$, for constants $c_0 = c_1 = 1$,

$$(a+b)^n = a + b = \sum_{k=0}^{n} c_k a^n b^{n-k}.$$

Suppose that, for some $n \in \mathbb{N}$, for some constants $c_{n,0}, c_{n,1}, \dots, c_{n,n}$,

$$(a+b)^n = \sum_{k=0}^{n} c_{n,k} a^k b^{n-k}.$$

Then,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) \\
&= \left(\sum_{k=0}^{n} c_{n,k} a^k b^{n-k}\right)(a+b) \\
&= \left(\sum_{k=0}^{n} c_{n,k} a^k b^{n-k}\right)a + \left(\sum_{k=0}^{n} c_{n,k} a^k b^{n-k}\right)b \\
&= \left(\sum_{k=0}^{n} c_{n,k} a^{k+1} b^{n-k}\right) + \left(\sum_{k=0}^{n} c_{n,k} a^k b^{n+(k-1)}\right) \\
&= \left(\sum_{k=0}^{n} c_{n,k} a^{k+1} b^{n-k}\right) + \left(\sum_{k=1}^{n} c_{n,k} a^k b^{n+(k-1)}\right) + c_{n,0}a^0 b^{n+1} \\
&= \left(\sum_{k=1}^{n+1} c_{n,k-1} a^k b^{n-(k+1)}\right) + \left(\sum_{k=1}^{n} c_{n,k} a^k b^{n+(k-1)}\right) + c_{n,0}a^0 b^{n+1}
\end{aligned}$$

$$\begin{aligned}
&= c_{n,n}a^{n+1}b^0 + \left(\sum_{k=1}^{n} c_{n,k-1}a^k b^{n-(k+1)}\right) + \left(\sum_{k=1}^{n} c_{n,k}a^k b^{n+(k-1)}\right) + c_{n,0}a^0b^{n+1} \\
&= c_{n,n}a^{n+1}b^0 + \left(\sum_{k=1}^{n} \left(c_{n,k-1}+c_{n,k}\right) a^k b^{n+(k-1)}\right) + c_{n,0}a^0b^{n+1} \\
&= \left(\sum_{k=0}^{n+1} \left(c_{n,k-1}+c_{n,k}\right) a^k b^{(n+1)+k}\right),
\end{aligned}$$

where $c_{n,-1} = c_{n,n+1} = 0$. Thus, letting $c_{n+1,k} = c_{n,k-1} + c_{n,k} \forall k \in \mathbb{N}$ with $0 \leq k \leq n+1$,

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} c_{n,k}a^kb^{(n+1)-k},$$

so, by the Principle of Mathematical Induction, the lemma is proven. ■

Exercise 29: Let G be a simple group of order 168, and, $\forall p \in \{3,5,7\}$, let n_p denote the number of Sylow p-subgroups of G.

a. By the Sylow theorems, $n_2|(3{\cdot}7) = 21, n_3|(2^3{\cdot}7) = 56, n_7|(2^3{\cdot}3) = 24$, and, as discussed in remark 11.6, since G is simple, $n_2, n_3, n_7 > 1$. Thus, $2 \in \{3,7,21\}, 3 \in \{2,4,7,8,14,28,56\}$, and $7 \in \{2,3,4,6,8,12,24\}$

Also by the Sylow theorems, $n_2 \cong 1 \pmod 2$, and $n_3 \cong 1 \pmod 3$, and $n_7 \cong 1 \pmod 7$, so $n_2 \in \{3,7,21\}, n_3 \in \{4,7,28\}$, and $n_7 = 8$. As noted in Remark 12.5, $n_2! \geq |G| = 168$ and $n_3! \geq |G| = 168$, so, since $3! = 6 < 168$ and $3! = 24 < 168$, $n_2 \neq 3$ and $n_3 \neq 4$. Thus, as desired, $n_2 \in \{7,21\}, n_3 \in \{7,28\}$, and $n_7 = 8$. ■

Exercise 31: Suppose R is a ring such that, $\forall r \in R$, $r^r = r$. Suppose $a,b \in R$. Then $(a+b) = (a+b)^2 = a(a+b) + b(a+b) = a^2 + ab + ba + b^2 = a + ab + ba + b$. Adding $(-a)$, $(-b)$, and $(-(ba))$ gives $ab = -ba = (-ba)^2$, so, by Lemma 1 (3), $ab = (ba)^2 = ba$, and so R is commutative. ■

Exercise 32: a. Let R be a commutative ring, with nilpotent elements $a,b \in R$. Then, $\exists n,m \in \mathbb{N}$ such that $a^n = b^m = 0$. Then, by Lemma 3, for some $c_0, c_1, \ldots, c_n \in \mathbb{N}$,

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} c_k a^k b^{(n+m)-k}.$$

Note that, $\forall k \in \mathbb{N}$ with $k \leq n+m$, either $k \geq n$ or $n+m-k \geq m$. Thus, by Lemma 1, for such k, $a^kb^{n+m-k} = 0b^{n+m-k} = 0$ or $a^kb^{n+m-k} = a^k0 = 0$, so

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} 0 = 0.$$

Thus, $(a+b)$ is nilpotent. ■

This does not hold if the R is non-commutative. Consider, for instance, $\mathcal{M}_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries. Then, for

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \; A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } B^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but

$$(A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

so that, as is seen by induction on n, $\forall n \in \mathbb{N}$,

$$(A+B)^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ or } (A+B)^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus, $A \in \mathcal{M}_2(\mathbb{Z})$ and $B \in \mathcal{M}_2(\mathbb{Z})$ are nilpotent, but $(A+B) \in \mathcal{M}_2(\mathbb{Z})$ is not nilpotent. ■

b. Let R be a commutative ring, with $a, r \in R$ and a nilpotent. Then, $\exists n \in \mathbb{N}$, such that $a^n = 0$, so that, by Lemmas 1 and 2, $(ar)^n = a^n r^n = 0r^n = 0$. Thus, (ar) is nilpotent. ■

This does not hold if the R is non-commutative. Consider, for instance, $\mathcal{M}_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries, and let A and B be as in the example in part a. Then,

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

and so, as is seen by induction on n, $\forall n \in \mathbb{N}$,

$$(AB)^n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus, as shown in part a., $A \in \mathcal{M}_2(\mathbb{Z})$ and $B \in \mathcal{M}_2(\mathbb{Z})$ are nilpotent, but $AB \in \mathcal{M}_2(\mathbb{Z})$ is not nilpotent. ■

Exercise 33: Let J be the set of polynomials $\{a_0 + a_1 x + \ldots \in \mathbb{Z}[x] : a_0 \equiv 0 \pmod 6, a_1 \equiv \pmod 3\}$. Suppose $A, B \in J$, with $A(x) = a_0 + a_1 x + \ldots, B(x) = b_0 + b_1 x + \ldots$. Clearly, since $a_0 + b_0 \equiv 0 + 0 \pmod 6 \equiv 0 \pmod 6$ and $a_1 + b_1 \equiv 0 + 0 \pmod 3 \equiv 0 \pmod 3$, J is closed under addition. Furthermore, the additive inverse of A is clearly in A, since $-a_0 \equiv -0 \pmod 6 \equiv 0 \pmod 6$, and $-a_1 \equiv -0 \pmod 3 \equiv 0 \pmod 3$. The identity polynomial has only zero coefficients, so it is clearly in J. Finally, since polynomial addition is associative, J is associative under addition, so J is a subgroup of $\mathbb{Z}[x]$ under addition.

If, on the other hand, $B \in \mathbb{Z}[x]$ but not necessarily $B \in J$, then, noting that polynomial multiplication is commutative, $(BA)(x) = (AB)(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots$, so J is an ideal of $\mathbb{Z}[x]$. ■

Suppose, for sake of contradiction, that $\mathbb{Z}[x]$ were a Principal Ideal Domain. Then, $\exists A \in J$ such that $(A) = J$. Since $\mathbb{Z}[x]$ is commutative and unital, $(A) = \{PA : P \in \mathbb{Z}\}$. Suppose that, for some $n \in \mathbb{N}$ with $n \geq 2$, $a_n \neq 0$. Then, $\forall P \in \mathbb{Z}[x]$, P has a nonzero coefficient besides those of its constant and linear terms, so, for $B(x) = 6$, $B \in J$ but $B \notin (A)$. Suppose, on the other hand, that $A = 6n_1 + 3n_2 x$, for some $n_1, n_2 \in \mathbb{Z}$. Then, 3 divides the coefficients of PA, so that, for $B(x) = x^2$, $B \in J$ but $B \notin (A)$. Thus, it must be the case that $(A) \neq J$, contradicting the choice of (A) as an element generating J. Therefore, $\mathbb{Z}[x]$ is not a Principal Ideal Domain. ■

Exercise 34: Let R be a ring, $\forall n \in \mathbb{N}$, let $\mathcal{M}_n(R)$ denote the set of $n \times n$ matrices with entries in R, let $\mathcal{J}$ be an ideal in $\mathcal{M}_n(R)$, and let J be the set of all values a such that a is the first entry of the first row of some matrix in $\mathcal{J}$. Note that it was stated in class that R may be assumed to be unital.

Since matrix addition is conducted element-wise, it is clear that J is a subgroup of R under addition because $\mathcal{J}$ is a subgroup of $\mathcal{M}_n(R)$.

Suppose $j \in J$, $r \in R$. Then, by definition of J, j is the first entry in the first row of some matrix $M \in \mathcal{J}$. Let A be the matrix with r in the first column of the first row, and 0 in all other entries. Then, JR has jr as the first entry of its first row, and RJ has rj as the first entry of its first row. Since $\mathcal{J}$ is an ideal, $RJ, JR \in \mathcal{J}$, so, by definition of J, $rj, jr \in J$. Thus, J is an ideal.

Suppose $A \in \mathcal{J}$, and let $a_{i,j} \in R$ be the value in the i^{th} row of the j^{th} column of A. Let $R_1 \in \mathcal{M}_n(R)$ be the matrix with 1 in the i^{th} column of its first row and 0 in all other entries, and let $R_2 \in \mathcal{M}_n(R)$ be the matrix with 1 in the first column of its j^{th} row. Then, $a_{i,j}$ is the entry in the first column of the first row of $R_1 A R_2$, so $a_{i,j} \in J$. Thus, all the entries in all of $\mathcal{J}$ are in J.

Suppose, on the other hand that A were an $n \times n$ matrix with entries in J. Then, matrices similar to R_1, R_2 above can be used to create from matrices in $\mathcal{J}$, a matrix whose j^{th} entry in its i^{th} is the same as that of A. This process can be repeated for each entry in A. Then, the sum of the resulting matrices is A, so, since $\mathcal{J}$ is an ideal and thus closed under both addition and multiplication by elements of $\mathcal{M}_n(R)$, $A \in \mathcal{J}$. Thus, all $n \times n$ matrices with entries in J are in $\mathcal{J}$. ■

Exercise 35: Let R be a commutative ring, with an ideal $J \subseteq R$.

a. Suppose $j \in Rad(J), r \in R$. Then, for some $n \in \mathbb{N}$, $j^n \in J$. Since $r^n \in R$ and J is an ideal, $j^n r^n, r^n j^n \in J$. Since R is commutative, by Lemma 2, $(jr)^n = j^n r^n$ so $rj = jr \in Rad(J)$.

Suppose $a, b \in Rad(J)$. Then, $\exists m, n \in \mathbb{N}$ such that $a^n, b^m \in J$. By Lemma 3, for some constants $c_0, c_2, \ldots, c_{n+m}$

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} c_k a^k b^{n+m-k}.$$

$\forall k \in \mathbb{N}$ with $k \leq n+m$, $k \geq n$ or $n+m-k \geq m$. Thus, for some $x, y \in \mathbb{N}$, $c_k a^k b^{n+m-k} = c_k a^x a^n b^y$ or $c_k a^x b^m b^y$. In either case, since J is an ideal, and thus closed under addition and multiplication by elements of R, $(a+b)^{n+m} \in J$, so $(a+b) \in Rad(j)$, and thus $Rad(J)$ is closed under addition. As noted in Remark 18.6, J is a subring of R. Thus, $0 \in J$, so, since $0^1 = 0$, $0 \in Rad(J)$. Since R is a ring and $Rad(J) \subseteq R$, $Rad(J)$ is both associative and commutative under addition. As a consequence of Lemma 1 (2) and (3), $\forall n \in \mathbb{N}$, $\forall a \in R$, (the proof is by induction on n using those lemmas, alternating on even and odd cases) $(-a)^n) = a^n$ or $(-a)^n = -(a^n)$. Thus, if $a^n \in J$, since J is a subgroup under addition, in either case, $(-a)^n \in J$, so $(-a) \in Rad(J)$. Thus, $Rad(J)$ subgroup of R under addition. Thus, $Rad(J)$ is an ideal. ■

Suppose $j \in Rad(Rad(J))$. Then, $\exists n \in \mathbb{N}$ such that $j^n \in Rad(J)$, so that $\exists m \in \mathbb{N}$ such that $(j^n)^m \in R$. Since $(j^n)^m = j^{nm}$ and $nm \in \mathbb{N}$, $j \in Rad(J)$. Suppose, on the other hand, that $j \in Rad(J)$. Then, for $n = 1$, $n \in \mathbb{N}$, and $j^n = j \in Rad(J)$, so $j \in Rad(Rad(J))$. Thus, $Rad(Rad(J)) = Rad(J)$. ■

b. Suppose $a_1 \in J_1, a_2 \in J_2, \ldots, a_m \in J_m$. Then, $\forall i \in \mathbb{N}$ with $1 \leq i \leq m$, since J_i is an ideal, for $a = a_1 a_2 \cdots a_i \cdots a_m$, $a \in J_i$. Since $\cap_{i=1}^m J_i$ is an ideal containing all elements of the form of a, it contains the smallest ideal generated by those elements, $J_1 J_2 \cdots J_m$ (i.e., $J_1 J_2 \cdots J_m \subseteq \cap_{i=1}^m J_i$). It follows immediately then that $Rad(J_1 J_2 \cdots J_m) \subseteq Rad(\cap_{i=1}^m J_i)$.

$\forall i \in \mathbb{N}$ with $1 \leq i \leq m$, $\cap_{k=1}^m J_k \subseteq J_i$, so $Rad(\cap_{i=1}^m J_k) \subseteq Rad(J_i)$, and thus $Rad(\cap_{i=1}^m J_k) \subseteq \cap_{i=1}^m Rad(J_k)$.

Suppose $j \in \cap_{i=1}^m Rad(J_i)$. Then, $\forall i \in \mathbb{N}$ with $1 \leq i \leq m$, $\exists n_i \in \mathbb{N}$ such that $j^{n_i} \in J_i$. Thus, for $n = \sum_{k=1}^m n_i$, $j^n = j^{n_1} j^{j_2} \cdots j^{n_m} \in J_1 J_2 \cdots J_m$. Thus, $j \in Rad(J_1 J_2 \cdots J_m)$, so $\cap_{i=1}^m Rad(J_i) \subseteq Rad(J_1 J_2 \cdots J_m)$.

Therefore, since $Rad(J_1 J_2 \cdots J_m) \subseteq Rad(\cap_{i=1}^m J_k) \subseteq \cap_{i=1}^m Rad(J_i) \subseteq Rad(J_1 J_2 \cdots J_m)$, $Rad(J_1 J_2 \cdots J_m) = Rad(\cap_{i=1}^m J_k) = \cap_{i=1}^m Rad(J_i)$. ■