Shashank Singh
sss1@andrew.cmu.edu
21-373 Honors Algebraic Structures, Fall 2011
Assignment 7
Due: Friday, November 11
Extension granted until Saturday, November 12

Exercise 43: i. Suppose, for sake of contradiction, that $2\mathbb{Z}$ and $3\mathbb{Z}$ were isomorphic, so that there exists an isomorphism $f : 2\mathbb{Z} \to 3\mathbb{Z}$. Note that, $\forall x \in \mathbb{Z}$, $2x = x^2$ if and only if $x = 0$ or $x = 2$, and that $f(2) \neq 0$, since f is bijective, and $f(0) = 0$ (because $f(0) = f(0) = f(0) + f(0)$). Thus, since f is an isomorphism, $f(2)+f(2) = f(2+2) = f(4) = f(2*2) = f(2)*f(2)$, so that $\exists x = f(2) \in 3\mathbb{Z}$. However, since $x \neq 0$, $x = 2$, contradicting the choice of $x \in 3\mathbb{Z}$. Thus, $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. ■

ii. Suppose, for sake of contradiction, that $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ were isomorphic, so that there exists an isomorphism $f : \mathbb{Q} \to \mathbb{Z}$. Note that no element of $\mathbb{Z}$ (except 1) is a unit and that no non-zero element of $\mathbb{Z}$ is nilpotent, and thus, by the result of Exercise 37 (from Assignment 6), $\forall P \in \mathbb{Z}[]$, P is a unit if and only if $P = 1$. Then, since f is an isomorphism, $1 = f(1) = f(2 * 2^{-1}) = f(2)f(2^{-1})$. However, this implies that $f(2)$ is a unit in $\mathbb{Z}[x]$, which is a contradiction, since $f(2) \neq 1$ (as f is a bijection, and $f(1) = 1$). ■

Exercise 44: i. Let $J \subseteq \mathbb{Z}$ be the set of polynomials $P \in \mathbb{Z}[x]$ such that P has a constant term which is a multiple of 3. Then, for $P \in \mathbb{Z}[x]$, $P \in J$ if and only if P can be written in the form $3n + xA$, for some $A \in \mathbb{Z}[x]$, $n \in \mathbb{Z}$. Thus, suppose $P, Q \in J$, with $P = 3m + xA$, $Q = 3n + xB$, for some $A, B \in \mathbb{Z}[x]$, $m, n \in \mathbb{Z}$. J inherits associativity and commutativity of addition and multiplication and distributivity of multiplication over addition from $\mathbb{Z}$. Since $0 = 3(0) + x(0)$, $0 \in J$. Since $-P = 3(-m) + x(-A)$, $(-P) \in J$. $P+Q = 3(m+n)+x(A+B)$, and $PQ = 3(3mn)+x(3mB+3nA+AB)$, $(P+Q), PQ \in J$. Suppose $C \in \mathbb{Z}[x]$, so that $C = k + xD$, for some $D \in \mathbb{Z}[x]$, $k \in \mathbb{Z}$. Then, $CP = PC = 3(mk) + x(3mD + kA + xAD) \in J$, so J is an ideal of $\mathbb{Z}[x]$. ■

ii. For $P, Q \in \mathbb{Z}[x]$ such that $P = 1$ and $Q = x^2$, P has a coefficient of x^2 which is a multiple of 3, but $PQ = x^2$ does not. Thus, the given set is not an ideal of $\mathbb{Z}[x]$. ■

iii. Let $J \subseteq \mathbb{Z}[x]$ be the set of polynomials $P \in \mathbb{Z}[x]$ such that the coefficients of the constant, linear, and quadratic terms of P are zero. Then, for $P \in \mathbb{Z}[x]$, $P \in J$ if and only if $P = x^3 A$, for some $A \in \mathbb{Z}[x]$. Thus, suppose $P, Q \in J$, with $P = x^3 A, Q = x^3 B$, for some $A, B \in \mathbb{Z}[x]$. J inherits associativity and commutativity of addition and multiplication and distributivity of multiplication over addition from $\mathbb{Z}$. $0 = x^3(0)$, so $0 \in J$. $-P = x^3(-A)$, so $(-P) \in J$. $P + Q = x^3(A + B)$, and $PQ = x^3(x^3 AB)$, so $(P + Q), PQ \in J$. Suppose $C \in \mathbb{Z}[x]$. Then, $CP = PC = x^3(AC) \in J$, so J is an ideal of $\mathbb{Z}[x]$. ■

iv. For $P, Q \in \mathbb{Z}[x]$ such that $P = 1$ and $Q = x$, only even powers of x appear in P, but an odd power of x appears in $PQ = x$. Thus, the given set is not an ideal of $\mathbb{Z}[x]$. ■

v. Let $J \subseteq \mathbb{Z}[x]$ be the set of polynomials $P \in \mathbb{Z}[x]$ such that the sum of all coefficients of P is zero. Then, for $P \in \mathbb{Z}[x]$, $P \in J$ if and only if $P(1) = 0$, so that $P = (x - 1)A$, for some $A \in \mathbb{Z}[x]$. Thus, suppose $P, Q \in J$, with $P = (x-1)A, Q = (x-1)B$, for some $A, B \in \mathbb{Z}[x]$. J inherits associativity and commutativity of addition and multiplication and distributivity of multiplication over addition from $\mathbb{Z}$. $0 = (x - 1)(0)$, so $0 \in J$. $-P = (x - 1)(-A)$, so $(-P) \in J$. $P + Q = (x - 1)(A + B)$, and $PQ = (x - 1)(x - 1)AB)$, so $(P + Q), PQ \in J$. Suppose $C \in \mathbb{Z}[x]$. Then, $CP = PC = (x - 1)(AC) \in J$, so J is an ideal of $\mathbb{Z}[x]$. ■

vii. For $P, Q \in \mathbb{Z}[x]$ such that $P = 1$ and $Q = x$, $P'(0) = 0$, but $(PQ)'(0) = 1 \neq 0$. Thus, the given set is not an ideal of $\mathbb{Z}[x]$. ■

Exercise 45: Let R be a commutative, unital ring, and, for some $n \in \mathbb{N}$, let $P_1, P_2, \ldots, P_n$ be prime ideals of R.

i. Let A be an ideal with the specified conditions. Since $a_2, a_3, \ldots, a_n \in A$ and A is an ideal and thus closed under multiplication, $a_2 a_3 \cdots a_n \in A$, and, since $a_1 \in A$ and A is closed under addition, $b = a_1 + a_2 a_3 \cdots a_n \in A$. Suppose, for sake of contradiction, that, for some $i \in \mathbb{N}$ with $2 \leq i \leq n$, $b \in P_i$. Since P_i is an ideal, $a_2 a_3 \cdots a_n \in P_i$. Thus, $(-a_2 a_3 \cdots a_n) \in P_i$, so $a_1 = (b + -a_2 a_3 \cdots a_n \in P_i$. his contradicts the choice of a_1 with $a_1 \notin A_i$. $\blacksquare$

ii. For $n = 1$, it follows trivially from $B \subset \bigcup_{i=1}^{n} P_i = P_1$ that $B \subset P_1$. Suppose, as an inductive hypothesis, that, for some $n \in \mathbb{N}$, $B \subset \bigcup_{i=1}^{n} P_i$ implies $B \subset P_i$, for some $i \in \mathbb{N}^*$. Suppose $B \subset \bigcup_{i=1}^{n+1} P_i$. If, for each $i \in \mathbb{N}$ with $1 \leq i \leq n+1$, $\exists a_i \in B \cap P_i$, then, as shown in part i., $\exists b \in B$ with $b \notin \bigcup_{i=1}^{n+1} P_i$, contradicting the choice of B. Otherwise, for some $i \in \mathbb{N}$ with $1 \leq i \leq n$, $B \cap P_i = \emptyset$, $B \subset \bigcup_{i=1}^{n} P_i$ (up to some re-indexing of $P_1, \ldots, P_{n+1}$), so that, by the inductive hypothesis, for some $i \in \mathbb{N}$ with $1 \leq i \leq n+1$, $B \subset P_i$. Thus, by the Principle of Mathematical Induction, $\forall n \in \mathbb{N}$, if $B \subset \bigcup_{i=1}^{n} P_i$ for prime ideals $P_1, P_2, \ldots, P_n$ of R, for some $i \in \mathbb{N}$ with $1 \leq i \leq n$, $B \subset P_i$. $\blacksquare$

Exercise 46: Let R be a ring with at least one non-zero element, and such that, for each non-zero $a \in R$, $\exists! b \in R$, written $b = \psi(a)$, such that $aba = a$.

i. Let $r, x, y \in R$, and let $b = \psi(r)$. If $rx = ry$, then $r(x - y) = 0$. Suppose, for sake of contradiction, that $x - y \neq 0$. Then, $b + (x - y) \neq b$. However, $r(b + (x - y))r = rbr + r(x - y)r = rbr + 0r = rbr = r$, which contradicts the given that $\psi(r)$ is unique. Thus, $x - y = 0$, so $x = y$. $\blacksquare$

ii. Suppose that, for some $a, b \in R$, $aba = a$. Then, $bab = babab$. By the result of part i., then, $b = bab$ (note that, as $\psi(a)$ is defined only for non-zero a, $a, b \neq 0$, and consequently, since $aba = a$, $ba \neq 0$, so that the result of part i. applies). $\blacksquare$

iii. Let non-zero $a \in R$. Let $c_1 = a\psi(a)$, $c_2 = \psi(a)a$, so that $ac_1 = a = c_1 a$, and let $b \in R$. Then, $ba = bc_1 a$, so that, by the result of part i., $b = bc_1$, and, similarly, $ab = ac_1 b$, so that $b = c_1 b$. Thus, c_1 is a mutiplicative identity in R. A similar proof shows that c_2 is a multiplicative identity of R, so that $c_1 = c_2$. Furthermore, $\forall r \in R$, $\psi(r)r = 1 = r\psi(r)$, so that every non-zero element of R has an inverse. Therefore, R is a division ring. $\blacksquare$

Exercise 47: Let p be an odd prime, let $R \subset \mathbb{Q}$ be the set of rationals whose denominators in reduced form are not divisible by p, and let $J \subset R$ be the set of such rational whose numerator in reduced form is a multiple of p.

i. Let $q, r \in R$, with $q = \frac{a}{b}$ and $r = \frac{c}{d}$, each in reduced form. Associativity and commutativity of addition and multiplication and distributivity of multiplication of over addition in R are inherited from $\mathbb{Q}$. Since, $0 = \frac{0}{1}$ in reduced form, and p does not divide 1, $0 \in R$. p does not divide b, so p does not divide the denominator of $-q = \frac{-a}{b}$. If p divided the denominator of either $p + q = \frac{ad+bc}{bd}$ or $pq = \frac{ac}{bd}$, then, by definition of prime, p would have to divide either b or d (noting that reducing a fraction can only eliminate factors of its denominator), which it does not, by choice of $p, q \in R$. Thus, since $R \subset \mathbb{Q}$, R is a subring of $\mathbb{Q}$.

Let $q, r \in J$, with $q = \frac{pa}{b}$ and $r = \frac{pc}{d}$. Associativity and commutativity of addition and multiplication and distributivity of multiplication of over addition in R are inherited from $\mathbb{Q}$. Clearly, since $0 = \frac{0}{1}$ in reduced form, $0 \in J$. Since $-p = \frac{-pa}{b}$, $(-p) \in J$. $p + q = \frac{pad+pcb}{bd}$, and $pq = \frac{p^2 ac}{bd}$, so $(p+q), pq \in J$ (as p does not divide bd, as explained above). Suppose $s \in R$, with $s = \frac{e}{f}$ in reduced form. Then $qs = \frac{pae}{bf}$. Since p does not divide bf, and p divides pae, $qs \in J$. Thus, since $J \subset R$, J is an ideal of R. $\blacksquare$

ii. Note that, $\forall i \in \mathbb{N}$ with $0 < n < p$, $\frac{1}{i} + \frac{1}{p-i} = \frac{p}{i(p-i)}$. Furthermore, since p is prime and $i, p - i < p$, $\frac{p}{i(p-i)}$ is in reduced form. The sum $\sum_{i=1}^{p-1} \frac{1}{i}$ can be re-written as $\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}$. Since the denominator of each term of the sum is not divisible by p, the denominator of the sum, which is the product of the denominators of the terms of the sum, in not divisible by p (as p is prime). Thus, p divides the numerator of the sum expressed in reduced form, so $\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \pmod{p}$. ■

Exercise 48: Let p be a prime greater than 3, and $k = \lfloor \frac{2p}{3} \rfloor$. Let $b = \sum_{i=1}^{k} \binom{p}{i}$. p^2 divides b if and only if $\frac{b}{p} \equiv 0 \pmod{p}$. Note that, by definition of the binomial coefficient,

$$\frac{b}{p} = \sum_{i=1}^{k} \frac{(p-1)(p-2)\cdots(p-(i-1))}{(1)(2)\cdots(i)} \equiv \sum_{i=1}^{k} \frac{(-1)(-2)\cdots(-(i-1))}{(1)(2)\cdots(i)} \pmod{p} = \sum_{i=1}^{k} \frac{(-1)^{i+1}}{i}$$

Since p is a prime greater than 3, either $p \equiv 1 \pmod{6}$ or $p \equiv 5 \pmod{}$ (since, otherwise, it would be divisible by either 2 or 3). In the first case, for some $n \in \mathbb{N}$, $p = 6n + 1$ and $k = 4n$, so that, letting $m = \frac{k}{2} + 1$, $m = 2k + 1$. In the second case, let for some $n \in \mathbb{N}$, $p = 6n + 5$ and $k = 4n + 3$, so that, letting $m = \frac{k+1}{2}$, $m = 2n + 2$. In either case, $m = p - (k + 1)$, so that $p - m = k + 1$. Furthermore, by this choice of m, adding and subtracting twice the sum of the even terms of the sequence gives:

$$\frac{b}{p} = \sum_{i=1}^{k} \frac{1}{i} - 2\sum_{i=1}^{m} \frac{1}{2i} = \sum_{i=1}^{k} \frac{1}{i} - \sum_{i=1}^{m} \frac{1}{i} = \sum_{i=1}^{k} \frac{1}{i} + \sum_{i=1}^{m} \frac{1}{(-i)} \equiv \sum_{i=1}^{k} \frac{1}{i} + \sum_{i=1}^{m} \frac{1}{(p-i)} \pmod{p} = \sum_{i=1}^{p-1} \frac{1}{i}$$

Then, by the result of part ii. of Exercise 47, $\frac{b}{p} \equiv 0 \pmod{p}$. ■