MATH 320 S26, Exam 2 Solutions

Questions 1-5 below refer to the ring B. Here the "numbers" are the subsets of $\{x, y\}$; there are four numbers altogether. For $a, b \in B$, we define multiplication as $a \times b = a \cap b$, i.e. the intersection of a and b. We define addition as $a + b = a \Delta b$. This is the symmetric difference of a and b, which you will recall is the set $\{z : (z \in a \wedge z \notin b) \vee (z \in b \wedge z \notin a)\}$ or if you prefer the set $(a \cup b) \setminus (a \cap b)$. You may use without proof basic set theory properties (e.g., $\cap$ and Δ are each commutative and associative).

B is called a Boolean ring. Although our exam had $|B| = 2$, we can build one of any size, using the same two operations. They can be used to model propositional calculus ($b \in B$ represents the set of propositions that are true).

1. Write out the addition and multiplication tables for B. (this proves closure)

$+$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x, y\}$
$\emptyset$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x, y\}$
$\{x\}$	$\{x\}$	$\emptyset$	$\{x, y\}$	$\{y\}$
$\{y\}$	$\{y\}$	$\{x, y\}$	$\emptyset$	$\{x\}$
$\{x, y\}$	$\{x, y\}$	$\{y\}$	$\{x\}$	$\emptyset$

$\times$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x, y\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{x\}$	$\emptyset$	$\{x\}$	$\emptyset$	$\{x\}$
$\{y\}$	$\emptyset$	$\emptyset$	$\{y\}$	$\{y\}$
$\{x, y\}$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x, y\}$

2. Find 0_B, find 1_B (if it exists), and determine whether B is commutative. Justify your answers.
   $0_B = \emptyset$, because (for any $a \in B$) $\emptyset + a = \emptyset \Delta a = (\emptyset \cup a) \setminus (\emptyset \cap a) = a \setminus \emptyset = a$.
   $1_B = \{x, y\}$, because (for any $a \in B$) $\{x, y\} \times a = \{x, y\} \cap a = a$.
   B is commutative, because (for any $a, b \in B$) $a \times b = a \cap b = b \cap a = b \times a$.
   (the middle step uses commutativity of $\cap$)

3. Prove that B is a ring, EXCEPT don't prove distributivity. You may use the results of the previous two problems.
   The previous problems proved closure and existence of 0_B. Now, let $a, b, c \in B$ be arbitrary.

   (associativity) $(a + b) + c = (a + b)\Delta c = (a \Delta b)\Delta c = a \Delta (b \Delta c) = a \Delta (b + c) = a + (b + c)$, and $(a \times b) \times c = (a \times b) \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap (b \times c) = a \times (b \times c)$.
   In the middle of each we used the associativity of Δ and $\cap$ (basic set theory properties)

   (commutativity of $+$) $a + b = a \Delta b = b \Delta a = b + a$, where we used commutativity of Δ.

   (inverses of $+$) For $x \in B$, it turns out that we can take $(-x) = x$, because $x + x = x \Delta x = \emptyset = 0_B$.

   (distributivity) This is a bit messy, and involves more set theory than is reasonable to expect you to remember for this exam. It is true though!

4. Find all units and zero divisors of B. Determine whether this ring is an integral domain. Determine whether this ring is a field. Determine whether this ring is cancellative.
   Both $\{x\}$ and $\{y\}$ are zero divisors, since they are nonzero and their product is zero (i.e. $0_B = \emptyset$). Since zero divisors can't be units (by exercise 2.10), and neither can zero (by definition of zero divisor), the only candidate to be a unit is $\{x, y\}$. This is indeed a unit, in fact it is 1_B.

   Because there are zero divisors, this ring is not an integral domain. Because it's not an integral domain, it is not a field. This ring is not cancellative, because $\{x\} \times \emptyset = \{x\} \times \{y\}$ (both sides equal $\emptyset$), yet if we cancelled $\{x\}$ we find that $\emptyset \neq \{y\}$. OR: By exercise 2.13, B isn't cancellative since it's commutative, has an identity, and is an integral domain.

5. Consider B', the subsets of $\{x\}$. Note that $B' \subseteq B$. Prove or disprove that B' is a subring of B.
   The statement is true. Note that $B' = \{\emptyset, \{x\}\}$. There are several things to check:

   (closure) Looking at the top left corners of the tables in problem 1 shows that if we restrict to $\emptyset, \{x\}$, the outcome will remain among $\emptyset, \{x\}$.

   (0_B) Since $0_B = \emptyset$, and this is in B', we find B' contains 0_B.

   (contains inverses) For every $a \in B$, in fact $(-a) = a$, so for sure if $a \in B'$ then $(-a) \in B'$.

6. Find, with justification, all the associates of [2] in $\mathbb{Z}_{12}$. How many are there?

To find the associates of [2], we need to multiply [2] by every possible unit. By exercise 2.6, we know that $[u]$ is a unit if and only if $\gcd(u, 12) = 1$. This happens exactly for $u = 1, 5, 7, 11$. Hence, the associates of [2] are $[1][2] = [2]$, $[5][2] = [10]$, $[7][2] = [14] = [2]$, and $[11][2] = [22] = [10]$. These include duplicates; in fact there are only two associates, namely [2] and [10].

7. Suppose that R is a ring with identity. Prove that this identity is unique.

Suppose 1_R and $1'_R$ were both identities of R. Because 1_R is an identity, for all $a \in R$, $a1_R = a$. In particular, taking $a = 1'_R$, we find that $1'_R 1_R = 1'_R$. Now, because $1'_R$ is an identity, for all $b \in R$, $1'_R b = b$. In particular, taking $b = 1_R$, we find that $1'_R 1_R = 1_R$. Combining these results, we find that $1'_R = 1'_R 1_R = 1_R$, so in fact $1'_R = 1_R$.

8. Let $p \in \mathbb{Z}$ with $p \geq 2$. Prove that p is prime, if and only if, $\mathbb{Z}_p$ is an integral domain.

We will prove the contrapositive in both directions, i.e. p is not prime, if and only if, $\mathbb{Z}_p$ is not an integral domain.

Suppose that p is not prime. By exercise 1.3, p is not irreducible. Hence we can factor $p = ab$, where $1 < a, b < p$. Now we have $[a][b] = [ab] = [p] = [0]$. Yet $[a], [b]$ are each nonzero, so we have zero divisors and therefore $\mathbb{Z}_p$ is not an integral domain.

Suppose that $\mathbb{Z}_p$ is not an integral domain. Now we have nonzero $[a], [b]$ such that $[a][b] = [ab] = [0]$. Because $[ab] = [0]$, we apply exercise 1.16 to conclude $ab \equiv 0 \pmod{p}$. Hence $p|ab$. However, $p \nmid a$ since otherwise $a \equiv 0 \pmod{p}$ and then $[a] = [0]$ (by exercise 1.16), which we assumed did not hold. Similarly, $p \nmid b$ since otherwise $b \equiv 0 \pmod{p}$ and then $[b] = [0]$ (by exercise 1.16), which we assumed did not hold. We have proven $p|ab$ and $p \nmid a$ and $p \nmid b$. This proves that p is not prime.

9. Let R be a commutative, cancellative, ring with identity. Prove that every prime is irreducible.

Let p be a prime, and suppose that a is a divisor of p. Then there is some $b \in R$ with $p = ab$. Hence $p1_R = ab$, so $p|ab$. Because p is prime, either $p|a$ or $p|b$.

If $p|a$, then there is some $k \in R$ with $pk = a$. Substituting, we get $p1_R = (pk)b = p(kb)$. Cancelling p from both sides, we get $1_R = kb$, so b is a unit. Multiplying $p = ab$ on both sides by b^{-1} we get $pb^{-1} = abb^{-1} = a1_R = a$, so a is an associate of p. Hence, each of a, b is either a unit or an associate of p.

If $p|b$, things are very similar. There is some $k \in R$ with $pk = b$. Substituting, we get $p1_R = a(pk) = (ap)k = (pa)k = p(ak)$. Cancelling p from both sides, we get $1_R = ak$, so a is a unit. Multiplying $p = ab$ on both sides by a^{-1} we get $a^{-1}p = a^{-1}ab = 1_R b = b$, so b is an associate of p. Again, each of a, b is either a unit or an associate of p.

10. Consider the ring $S = \mathbb{Z}[\sqrt{-5}]$. Prove that $3 = 3 + 0\sqrt{-5}$ is irreducible and not prime.

We rely on the norm function from exercise 2.19: $N(a+b\sqrt{-5}) = a^2+5b^2$, which is multiplicative and satisfies $N(x) = 1$ iff x is a unit. Note that $N(3) = 9$.

If 3 were reducible, then $3 = xy$ where $N(x) = N(y) = 3$ (since 3×3 is the only way to factor 9 apart from 1×9). However, there is no $x = a + b\sqrt{-5}$ with $N(x) = 3$, which we will prove in the lemma below. This proves that 3 is irreducible.

Now, set $u = 1 + 1\sqrt{-5}, v = 1 - 1\sqrt{-5}$. Note that $N(u) = N(v) = 6$. We have $2 \times 3 = 6 = u \times v$, so $3|uv$. If 3 were prime, then $3|u$ or $3|v$. But then, since the norm is multiplicative, either $N(3)|N(u)$ or $N(3)|N(v)$, i.e. 9|6 or 9|6, neither of which holds. Hence 3 is not prime.

Lemma: There is no $x = a + b\sqrt{-5}$ with $N(x) = 3$.
Proof: Suppose otherwise. If $|b| > 0$, then $N(x) \geq 5|1|^2 = 5 > 3$, so $b = 0$ and $x = a + 0\sqrt{-5}$. But now $N(x) = a^2$. If $|a| \leq 1$ then $N(x) \leq 1$; if $|a| \geq 2$ then $N(x) \geq 4$. Either way we get a contradiction.