MATH 315 WEEK 1

JACOB TERKEL

2023

Problem 6, Chapter 13

Claim. *Let $a * b = a + b + 1$, and $a \diamond b = ab + a + b$ be operations on $\mathbb{R}$. All axioms are satisfied.*

Proof.

($*$ Clos) We know that the real numbers are closed under addition and so for any real a and b the quantity $a * b = a + b + 1$ is real, and so $*$ has the closure property.

($*$ Comm) To show that $*$ is commutative we need to show that $a * b = b * a$. This is easily seen the be true as $a * b = a + b + 1 = b + a + 1 = b * a$.

($*$ Asso) To show that $*$ is associative we need to show that $(a * b) * c = a * (b * c)$. This can be demonstrated to hold as follows

$$(a * b) * c =$$

$$(a + b + 1) * c = a + b + c + 1 + 1 = a + (b + c + 1) + 1 = a * (b + c + 1)$$

$$= a * (b * c).$$

($*$ Id) To show that $*$ has the identity property, we must demonstrate that there exists some $b \in \mathbb{R}$, such that $a * b = b * a = a$, for all $a \in \mathbb{R}$. Because we showed that $*$ commutes it suffices to show that $a * b = a$. Now, observe that $-1 \in \mathbb{R}$ and for $a \in \mathbb{R}$ we have that $a * -1 = a * -1 + 1 = a$, thus $*$ satisfies identity.

($*$ Inv) As shown above, $*$ satisfies identity with identity being -1. Thus the inverse of a real number a exists if there is a real number b satisfying $a + b + 1 = -1$ which can be seen to be equivalent to $b = -2 - a$, and because a is a real number, b is real thus inverse is satisfied.

(⋄ Clos) This follows from the fact that multiplication and addition satisfy closure on $\mathbb{R}$. As $a \diamond b = ab + a + b$ and so because a and b are real it follows that ab is real, and from this $ab + a + b$ is real.

(⋄ Comm) Similar to above, we demonstrate this by showing that $a \diamond b = b \diamond a$. This is done as follows

$$a \diamond b = ab + a + b = ba + b + a = b \diamond a.$$

(⋄ Asso) To show that $\diamond$ satisfies the associative property we must show that $(a \diamond b) \diamond c = a \diamond (b \diamond c)$. This is true, as we can show as follows

$$(a \diamond b) \diamond c = (ab + a + b)c + (ab + a + b) + c = abc + ac + ac + ab + a + b + c =$$

$$a(bc + b + c) + (bc + b + c) + a = a \diamond (bc + b + c) = a \diamond (b \diamond c).$$

(⋄ Id) We show that $\diamond$ has the identity property by demonstrating that there is some $b \in \mathbb{R}$ for which $a \diamond b = b \diamond a = a$ for all $a \in \mathbb{R}$. Note that because $\diamond$ is commutative we need only show that $a \diamond b = a$. I claim the 0 satisfies this property. Indeed, 0 is a real number and that $a \diamond 0 = a \cdot 0 + a + 0 = a$, and thus $\diamond$ satisfies identity.

(⋄ Inv) We know that $\diamond$ satisfies the identity property, and thus to show that $\diamond$ satisfies the non-zero inverse property we need only show that for all $a \in R \setminus \{-1\}$ there exists a real number b such that $a \diamond b = b \diamond a = 0$. We only need to show that $a \diamond b = 0$ as $\diamond$ is commutative. This is shown to be true as this is equivalent to $a \cdot b + a + b = 0$ which can be rearranged to $\frac{a}{a+1} = b$, and clearly $\frac{a}{a+1}$ is real for all real $a \neq -1$, and so $\diamond$ satisfies inverse.

(⋄ NZPP) To show that $\diamond$ has the non-zero product property we must show that if $a \diamond b = -1$ then one of a or b is -1. We show this as follows. We start with the equation

$$a \diamond b = -1.$$

We evaluate the $\diamond$ operation and we have that

$$a \cdot b + a + b = -1.$$

Upon doing some algebra we get that $(a+1)(b+1) = 0$ Which by the zero product property in $\mathbb{R}$ implies that either $a + 1$ or $b + 1$ is zero, in both cases, this shows that the non-zero product property is satisfied.

(⋄∗ Dist) Distributive is satisfied as $a \diamond (b * c) = a \diamond (b + c + 1) = a(b + c + 1) + b + c + 1 + a = ab + a + b + ac + a + c + 1 = (a \diamond b) + (a \diamond c) + 1 = (a \diamond b) * (a \diamond c)$

$\boxed{J\tau}$

Problem 8a, Chapter 13

Claim. *$D(6)$ is a boolean algebra.*

Proof.

($\overline{\text{Clos}}$) If d is a divisor of n then we have that there is an integer m such that $n = dm$, however, since d is an integer this means that m is also a divisor of n. Now, see that that $\overline{d} = \frac{n}{d} = m$, and as shown above m is a divisor of n proving $\overline{\ }$ closure.

($*$ Clos) We show this by demonstrating that for any two factors of n, a and b, that $\text{lcm}(a, b)$ is a factor of n. By the fundamental theorem of arithmetic, we have the following:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod p_i^{\alpha_i}$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod p_i^{\beta_i}.$$

We can see that

$$\text{lcm}(a, b) = \prod p_i^{\max(\alpha_i, \beta_i)}.$$

However, Note that n must also have prime factorization

$$n = \prod p_i^{c_i},$$

Furthermore, observe that a number m is a factor of n if and only if $m = p_1^{\mu_i} p_2^{\mu_2} \cdots p_k^{\mu_k}$ and $\mu_i \leq c_i$ for all i. Now see that because a and b are factors of n we have $c_i \geq \alpha_i$ and $c_i \geq \beta_i$ which means $c_i \geq \max(a_i, b_i)$ for all i. This means that $\text{lcm}(a, b)$ is also a factor of n.

($*$ Comm) It is obvious that $\text{lcm}(a, b) = \text{lcm}(b, a)$. From the maximum definition used above as $\max(a, b) = \max(b, a)$.

($*$ Asso) To show this we must show that $\text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(\text{lcm}(a, b), c)$. We use the fundamental theorem of arithmetic to say that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod p_i^{\alpha_i},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod p_i^{\beta_i},$$

and

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} = \prod p_i^{\gamma_i}.$$

We get that

$$\text{lcm}(a, \text{lcm}(b, c)) = \prod p_i^{\max(a, \max(b, c))}$$

and

$$\text{lcm}(\text{lcm}(a, b), c) = \prod p_i^{\max(a, \max(b, c))}$$

which are both clearly equal to

$$\prod p_i^{\max(a, b, c)}$$

as the maximum function is clearly associative.

(∗ Id) Clearly, 1 is a divisor of n and for any divisor of n, a, we have that $\text{lcm}(a, 1) = \text{lcm}(1, a) = a$.

(⋄ Clos) This one is easy as for any pair of divisors of a and b of n we have that $\gcd(a, b)$ is a divisor of a by definition, and a divides n, thus $\gcd(a, b)$ divides n.

(⋄ Comm) Similarly to how we defined lcm we can define gcd as follows in terms of two divisors a and b.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod p_i^{\alpha_i},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod p_i^{\beta_i},$$

we have that

$$\gcd(a, b) = \prod p_i^{\min(\alpha_i, \beta_i)}.$$

, and because $\min(a, b) = \min(b, a)$ we have that, gcd is commutative.

(⋄ Asso) The proof for ⋄ associativity is nearly identical to ∗ Associativity.

(⋄ Id) Clearly n is a factor of n, and it is also evident that $\gcd(n, a) = \gcd(a, n) = a$ for all $a \in D(n)$.

(∗⋄ Comp) The complement pairs in $D(6)$ are $\{1, 6\}$ and $\{2, 3\}$. We see that $1 * 6 = 2 * 3 = 6 = \text{Id}_\diamond$, thus ∗⋄ complementation is satisfied.

(⋄∗ Comp) The complement pairs in $D(6)$ are $\{1, 6\}$ and $\{2, 3\}$. We see that $1 \diamond 6 = 2 \diamond 3 = 1 = \text{Id}_*$, thus ⋄∗ complementation is satisfied.

(⋄∗ Dist) To show this we must show that $a * (b \diamond c) = a * b \diamond a * c$, or equivalently $\text{lcm}(a, \gcd(b, c)) = \gcd(\text{lcm}(a, b), \text{lcm}(a, c))$. Using the maximum and minimum definitions we have utilized thus far and the following factorizations for a, b, and c:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod p_i^{\alpha_i},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod p_i^{\beta_i},$$
$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} = \prod p_i^{\gamma_i}.$$

We have that

$$\text{lcm}(a, \gcd(b, c)) = \prod p_i^{\max(a, \min(b, c))}.$$

The quantity $\max(a, \min(b, c))$ will be equal to a if a is greater either of b or c, and will be equal to the small of b and c if they are both greater than a. Now, look at the quantity $\min(\max(a, b), \max(a, c))$. It is easily seen that the above quantity can be identically described and so we have that they are equal. This gives us

$$\text{lcm}(a, \gcd(b, c)) = \prod p_i^{\max(a, \min(b, c))} = \prod p_i^{\min(\max(a, b), \min(a, c))} = \gcd(\text{lcm}(a, b), \text{lcm}(a, c)).$$

(∗⋄ Dist) This proof is nearly identical to the above, and I will not be repeating it, sorry!

$\boxed{J\tau}$

Problem 8b, Chapter 13

Claim. *$D(8)$ is not a boolean algebra.*

Proof. We can see that $e_\diamond = 1$. Note that for $a = 2$ we have that $a * \bar{a} = 2$, and thus complementation does not hold. $\boxed{J\tau}$

Problem 8c, Chapter 13

Conjecture 1. *$D(n)$ a boolean algebra if and only if n is squarefree.*

Problem 9a, Chapter 13

Definition 1. The negative elements of a ring, R, with positive elements P is defined to be $N = \{-x \mid x \in P\}$.

Alternatively, $N = R \setminus (P \cup \{0\})$.

Problem 9b, Chapter 13

Claim. *For a pair of elements a and b in an ordered ring R with positive set P and negative set N we define the following order relations.*

($\geq$) $a \geq b$ *if* $a - b \in P \cup \{0\}$.
($\leq$) $a \leq b$ *if* $a - b \in N \cup \{0\}$.
($>$) $a > b$ *if* $a - b \in P$.
($<$) $a < b$ *if* $a - b \in N$

Problem 9e, Chapter 13

Claim. *$\mathbb{Z}_n$ can never be an ordered ring for $n \geq 2$*

Proof. Assume that there is some $n \geq 2$ for which $\mathbb{Z}_n$ is an ordered ring. Because $n \geq 2$, 1 and $n-1$ are non-zero elements in $\mathbb{Z}_n$, and because $1 = -(n-1)$ at exactly one of 1 or $n-1$ is an element of P. However, if it is 1 that is the element of P we have that $\sum_{i=1}^{n-1} 1 = n - 1$

but by axiom $O+$ this would imply that $n-1$ is also an element of P which cannot be. The same thing occurs if we assume that $n-1$ is an element of P as $\sum_{i=1}^{n-1} n-1 = n^2-2n+1 = 1$. Thus, neither 1 nor $n-1$ are elements of P which cannot be if $\mathbb{Z}_n$ is an ordered ring. $\boxed{J\tau}$

Problem 10a, Chapter 13

Claim. *τ_n is a topology for all n.*

(a) The empty set is in τ_n vacuously. S is also in τ_n as we can reword the condition to be in τ_n as follows: U is in τ_n if it is a subset of S that contains every positive multiple of its elements less than or equal to n. And because S contains every positive integer less than or equal to n, $S \in \tau_n$.

(b) Using the same reworded condition as before, it is clear that for a pair of $A, B \in \tau_n$ any element in $A \cap B$ satisfies the condition that if $m \in A \cap B$ then every multiple of m less than n is in $A \cap B$. This can be seen to be true as if $m \in A$ and $m \in B$ because $A, B \in \tau_n$ we have that every multiple of m less than n is also in A and B, and thus their intersection. Thus, we have that $A, B \in \tau_n \implies A \cap B \in \tau_n$.

(c) A slightly modified version of the above argument suffices for this part.

Problem 10b, Chapter 13

Claim.

$$\tau_1 = \{\emptyset, \{1\}\}$$

$$\tau_2 = \{\emptyset, \{1,2\}, \{2\}\}$$

$$\tau_3 = \{\emptyset, \{1,2,3\}, \{2,3\}, \{2\}, \{3\}\}$$

$$\tau_4 = \{\emptyset, \{1,2,3,4\}, \{2,4\}, \{3,4\}, \{2,3,4\}, \{3\}, \{4\}\}$$

$$\tau_5 = \left\{ \begin{array}{c} \emptyset, \{5\}, \{4\}, \{3\}\{4,5\}, \{3,5\}, \{3,4\}, \{3,4,5\} \\ \{2,3,4\}, \{2,4,5\}, \{2,3,4,5\}, \{1,2,3,4,5\} \end{array} \right\}$$

$$\tau_6 = \left\{ \begin{array}{c} \emptyset, \{6\}, \{5\}, \{4\}, \{5,6\}\ \{4,6\}, \{4,5\}, \{3,6\}, \\ \{2,4,6\}, \{3,5,6\}, \{4,5,6\}, \{3,4,6\}, \{3,4,5,6\} \\ \{2,3,4,6\}, \{2,4,5,6\}, \{2,3,4,5,6\}, \{1,2,3,4,5,6\} \end{array} \right\}$$

Problem 11, Chapter 13

Claim. *Let $\mathcal{P}$ and $\mathcal{L}$ constitute projective plane. There exists a natural number n with the property that every line in $\mathcal{L}$ includes exactly $n+1$ points, every point in $\mathcal{P}$ is on $n+1$ lines, and $|\mathcal{L}| = |\mathcal{P}| = n^2 + n + 1$.*

Proof. Let $\mathcal{P}$ and $\mathcal{L}$ be points and lines for some projective plane. We know by (P1) that there are at least two different lines. Because they are different lines there is a pair of points p_1 and p_2 in $\mathcal{P}$ that are on one line but not the other, but because each pair of points lie on a line, there is a third line that includes those two points, as well as some other point not on the previous two lines as every line must contain three or more points (P2), as for any pair of points there is exactly one line that contains both.

Thus there exists a line L_1 and a point P such that P is not on L. For each point on L, p_i, there exists exactly one line containing both p_i and P by (P4). Furthermore, if ℓ^P is some line containing P, by (P5) there is a unique point that is on both L and ℓ^P. This gives us a bijection between the points on L and the lines that go through P. The above can be done for any pair of line and point not on that line. However, recall that for any pair of lines we showed that there is a point $\mathbf{p}$ not on either of those lines.

By the above, the number of points on both of those lines must be equal to the number of lines that go through $\mathbf{p}$. Let this natural number be k. However, note that we can select one of these lines, ℓ_1 as well as any other line ℓ^* in the projective plane and we have that there is a point $\mathbf{p}^*$ on neither of those lines. From this, we have that the number of points that go through p^* is the same as the number of points that are on ℓ_1, which in turn will be the number of points on ℓ^*. From this, it follows that every line will have k points on it. Furthermore, since there is no line with every point, the number of points on a line and the number of lines that go through each point are equal.

Now, consider some point $p \in \mathcal{P}$. We have that k lines pass through p. Furthermore, every point in $\mathcal{P}$ is on one of those lines as for any pair of points there is a unique line that passes through both (P4). Furthermore, each point, with the exception of p, can only lie on one of these lines as for any pair of lines there is exactly one point that lies on both lines (P5). Thus, because each of these lines includes exactly k points we have that $|\mathcal{P}| = k(k-1)+1$. By (P1), each line contains at least two points, and thus there exists a natural number n such that $k = n+1$ and we have that $|\mathcal{P}| = n(n+1)+1 = n^2+n+1$. Now, let w equal the total number of times any line intersects any point, it can be seen that $w = k|\mathcal{P}|$ and $w = k|\mathcal{L}|$. Thus, $|\mathcal{P}| = |\mathcal{L}|$. Thus, we have that $|\mathcal{P}| = |\mathcal{L}| = n^2+n+1$. $\boxed{J\tau}$

Remark. In this proof we utilized axioms P1, P2, P4, and P5, but not P3. Recall that in chapter four we proved that P3 is not independent of the other four axioms, and thus it should never be required to prove any statement regarding projective planes.