Exercise 8

Discrete Mathematics

November 26, 2020

Exercise 71

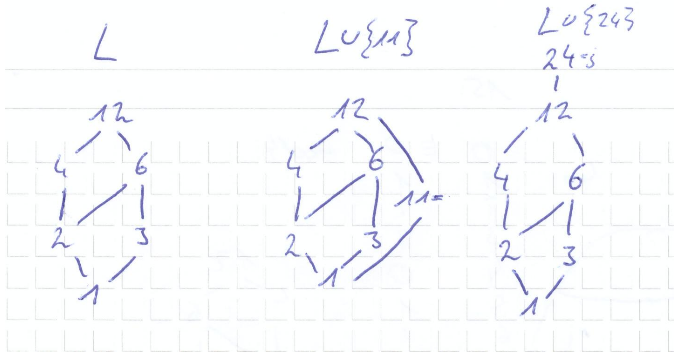
$x \wedge y$ ("meet") is the unique maximal element of all common lower elements of x, y if it exists. $x \vee y$ ("join") is the unique minimal element of all common upper bounds of x, y if it exists. P is called a lattice if $x \wedge y, x \vee y$ exist for all $x, y \in P$.

a) $0 \in P$ is the zero-element if and only if $\forall x \in P : 0 \leq x$. $1 \in P$ is the one-element if and only if $\forall x \in P : x \leq 1$.

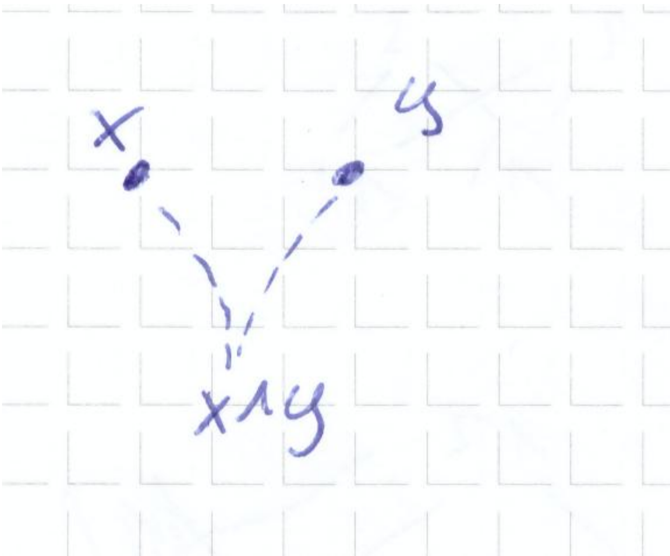
Proof by induction. $P(n)$: A lattice L of size n has a 0-element and a 1-element.

$P(1)$: By reflexivity holds for the only element $l \in L$ that $l \leq l$. Hence, x is zero-element and one-element.

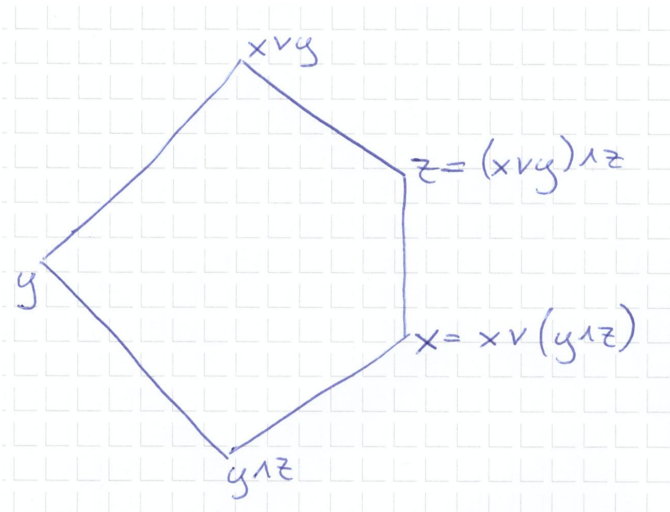
$P(n) \to P(n+1)$: Assume $P(n)$. Consider the lattice $L \cup \{j\}$ of size $n+1$. Then there is $x \wedge j$ and $x \vee j$ for all $x \in L \cup \{j\}$. Note that this holds for $x = 0$ and $x = 1$. That is, there exists $1 \vee j$ and $0 \wedge j$. Case 1: $1 \leq j$. Then j is the new 1 and 0 remains 0. Case 2: $0 \leq j \leq 1$. Then 1 and 0 remain equal. Case 3: $j \leq 0$. Then j is the new 0 and 1 remains 1.



b) $x \wedge y$ is a common lower bound of x and y. That means $x \wedge y \leq y$. $x \wedge y$ is a lower bound of y. Therefore, y is the smallest common upper bound of $x \wedge y$ and itself. Hence, by definition $y = y \vee (x \wedge y)$.



c) `https://en.wikipedia.org/wiki/Modular_lattice#Examples` Consider the following lattice.



We see that $x \leq y$, the hypothesis of the implication, holds. We also see that x and y are distinct. Note that $x = x \vee (y \wedge z)$ and $z = (x \vee y) \wedge z$. It follows

$x \vee (y \wedge z) \neq (x \vee y) \wedge z$. That means, the conclusion of the implication does not hold. Hence, the implication is wrong.

Exercise 73

1. Assume $\exists e \in \mathbb{Z} : b = ae, \exists f \in \mathbb{Z} : c = af$. Let x, y be arbitrary integers. Then $xb = aex$ and $yc = afy$. By addition we get $xb + yc = aex + afy = a(ex + fy)$ where $ex + fy$ is just another integer, say $z \in \mathbb{Z}$. Then $xb + yc = az$, so by definition $a \mid xb + yc$.

2. *Could be shorter and without the lemma*

   https://math.stackexchange.com/a/1920634

   Lemma: From $ma+nb = 1$ with $a, b, n, m \in \mathbb{Z}$ (linear combination of a, b) follows that a, b are coprime.
   Proof: Assume they are not coprime. Then there exists an integer $d > 1$ that divides a and b. Then there exist integers s, t such that $a = ds$ and $b = dt$. It follows
   $$ma + nb = 1 \Leftrightarrow m(ds) + n(dt) = 1 \Leftrightarrow d(ms + nt) = 1$$
   It follows that d divides 1. The only positive number that divides 1 is 1 itself, so $d = 1$. However, we previously had $d > 1$. Contradiction. Hence, a and b are coprime. This concludes the proof of the lemma.

   https://math.stackexchange.com/a/985209

   Assume $\gcd(a, b) = 1$ and $c \mid a$ and $d \mid b$. Then $\exists x \in \mathbb{Z} : a = xc$ and $\exists y \in \mathbb{Z} : b = yd$. Furthermore, Bézouts theorem implies $\exists e, f \in \mathbb{Z} : 1 = ae + bf$, from which follows by substitution $\exists e, f \in \mathbb{Z} : 1 = (xe)c + (yf)d$. As xe and yf are just integers, c and d are coprime, so by definition $\gcd(c, d) = 1$.

3. Assume $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$. Then by definition $\exists x \in \mathbb{Z} : c = xa$ and $\exists y \in \mathbb{Z} : c = yb$ and by Bézout's theorem $\exists e, f \in \mathbb{Z} : 1 = ae + bf$. Multiplying both sides by c gives $c = ace + bcf$ and by substituting c we get $c = a(yb)e + b(xa)f$. So we get $c = ab(ye + xf)$ where $ye + xf$ is an integer. Then by definition $ab \mid c$.

Exercise 74

For integers a, b holds $x = 2a + 1$ and $y = 2b + 1$. It follows

$$\begin{aligned} x^2 + y^2 &= (2a + 1)^2 + (2b + 1)^2 \\ &= 4(a^2 + a) + 1 + 4(b^2 + b) + 1 \\ &= 4z + 2 \end{aligned}$$

where $z = a^2 + a + b^2 + b$ is some integer. This means that $x^2 + y^2$ divided by 4 leaves remainder 2, that is $4 \nmid (x^2 + y^2)$. As x, y are odd it follows x^2, y^2 are odd which implies $x^2 + y^2$ is even, that is $2 \mid (x^2 + b^2)$.

Alternatively, consider $x^2 + y^2 = 4z + 2 = 2(2z + 1)$. As z can be any integer, $2z + 1$ is an odd integer. As $2z + 1$ is an integer, it follows again $2 \mid (x^2 + b^2)$. As it is additionally odd (and odd multiples of 2 are not divisble by 4), it follows again $4 \nmid (x^2 + y^2)$.

k	1	2	3	4	5	6	7	8	9
2k	2	4	6	8	10	12	14	16	18

Exercise 75

- Note that $n^2 - n = (n - 1)n$ is the product of two consecutive integers. One factor must be divisible by two. Therefore, the product is divisible by two. Hence, $n^2 - n$ is even.

- https://math.stackexchange.com/a/211122

  https://math.stackexchange.com/a/1359478

  Note that $n^3 - n = (n - 1)n(n + 1)$ is the product of three consecutive integers. One factor must be even and one must be a multiple of three. Hence, the product is a multiple of both 2 and 3. Therefore, it is divisble by by the least common mulitple of 2 and 3, which is 6.

Exercise 76

https://math.stackexchange.com/a/1114724

By definition, we have to show that $4 \mid (a + b) \wedge 4 \mid 4 \wedge (t \mid (a + b) \wedge t \mid 4 \implies t \mid 4)$. As $(t \mid (a + b) \wedge t \mid 4 \implies t \mid 4)$ is a tautology, what we have to show is

$$4 \mid (a + b)$$

From $\gcd(a, 4) = 2$ follows $a = 2k$ where k is odd. Otherwise the gcd would be 4.

k	1	2	3	4	5	6	7	8	9
a	2	4	6	8	10	12	14	16	18
$\gcd(a, 4)$	2	4	2	4	2	4	2	4	2

Likewise, from $\gcd(b, 4) = 2$ follows $b = 2m$ where m is odd. Hence, $a+b = 2(k+m)$. As for all odd numbers, the sum of $k+m$ is even. So for some integer x holds $k+m = 2x$, which yields $a + b = 2 \cdot 2x = 4x$. Therefore, we get the required property $4 \mid (a + b)$.

Exercise 77

Can also be calculated using the definitions of gcd and lcm

https://math.stackexchange.com/a/470827

We know Bézout's identity from the lecture:

$$d = \gcd(a, b) \implies \exists e, f \in \mathbb{Z} : d = ae + bf \tag{1}$$

Note that d divides ab. Let $m = \frac{ab}{d}$. To complete the proof, we show that m is the least common multiple of a and b. Certainly m is some multiple of a and b. Let n be any other common positive multiple of a and b. We show that m divides n. This will show that $m \leq n$, making m the least common multiple.

We have

$$\frac{n}{m} = \frac{nd}{ab} = \frac{n(ae + bf)}{ab} = \frac{n}{b}e + \frac{n}{a}f.$$

As we assumed n to be a multiple of a and b, the term $\frac{n}{b}e + \frac{n}{a}f$ is certainly an integer, and therefore n/m is an integer, too. Hence, n is a multiple of m.

From our initial assumption $m = \frac{ab}{d}$ follows the identity

$$md = ab$$

Exercise 78

$$\begin{aligned}
2863 &= 1057 \cdot 2 + 749 \\
1057 &= 749 \cdot 1 + 308 \\
749 &= 308 \cdot 2 + 133 \\
308 &= 133 \cdot 2 + 42 \\
133 &= 42 \cdot 3 + 7 \\
42 &= 7 \cdot 6 + 0
\end{aligned}$$

$$\begin{aligned}
7 &= 133 - 42 \cdot 3 \\
&= 133 - (308 - 133 \cdot 2) \cdot 3 = 7 \cdot 133 - 3 \cdot 308 \\
&= 7 \cdot (749 - 2 \cdot 308) - 3 \cdot 308 = 7 \cdot 749 - 17 \cdot 308 \\
&= 7 \cdot 749 - 17 \cdot (1057 - 749) = 24 \cdot 749 - 17 \cdot 1057 \\
&= 24 \cdot (2863 - 2 \cdot 1057) - 17 \cdot 1057 = 24 \cdot 2863 - 65 \cdot 1057
\end{aligned}$$

Multiply both sides by 6 to get

$$42 = 144 \cdot 2863 - 390 \cdot 1057$$

so $a = 144$ and $b = -390$. *You can also start the second/backwards part at the line* $308 = 133 \cdot 2 + 42$ *and avoid the multiplication by 6.*

Exercise 79

solver

$$
\begin{aligned}
x^3+5x^2+7x+3 &= \left(x^3+x^2-5x+3\right)1+\left(4x^2+12x\right)\\
x^3+x^2-5x+3 &= \left(4x^2+12x\right)\left(\frac{1}{4}x-\frac{1}{2}\right)+(x+3)\\
4x^2+12x &= (x+3)\,4x+(0)
\end{aligned}
$$

The GCD (last non-zero remainder) is $x+3$.

Calculation example: To calculate $\left(x^3+x^2-5x+3\right):\left(4x^2+12x\right)$ we start with $\frac{1}{4}x$ to adjust $4x^2$ to x^3. As $\left(x^3+x^2-5x+3\right)-\frac{1}{4}x\left(4x^2+12x\right)=-2x^2-5x+3$ has the same degree as $\left(4x^2+12x\right)$, we continue and add $-\frac{1}{2}$ to adjust $4x^2$ to $-2x^2$. The following division yields the remainder $x+3$. Then we are done with this line.

Exercise 80

Illustration of $n \equiv m \mod 4$:

n	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
m	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1

Assume to the contrary that there are only finitely many primes p with $p \equiv 3 \mod 4$. Let this set be $P=\{p_1,p_2,\dots,p_n\}$.

Let $a=4p_1p_2\dots p_a-1$. Then $a-(-1)=4p_1p_2\dots p_n$. Then $4 \mid a-(-1)$. By definition $x \equiv y \mod m \Leftrightarrow m \mid (x-y)$. Therefore, $a \equiv -1 \equiv 3 \mod 4$ (see table).

Only the product of two odd numbers gives an odd number. a is odd. Therefore, all prime divisors of a are odd. Let t be an arbitrary one of them. Then t must be of the form $4k+1$ or $4k+3$, and can certainly not be of the form $4k$ or $4k+2$ for some integer k. Hence, for for any prime divisor t of a holds $t \equiv 1 \mod 4$ or $t \equiv 3 \mod 4$.

Furthermore, there is at least one prime factor q of the prime factorization of a with $q \not\equiv 1 \mod 4$. Proof by contradiction: Suppose all prime factor of a are congruent to 1 modulo 4. Then they are of the form $4m+1$. Notice that the product of two such prime factors $(4m+1)(4k+1)=4(4km+k+m)+1$ is of the same form. By induction, the product of all prime factors of a is of that form. So a itself is of that form, and hence $a \equiv 1 \mod 4$. But we have shown that $a \equiv 3 \mod 4$. Contradiction. Therefore, $q \not\equiv 1 \mod 4$. By our previous result follows $q \equiv 3 \mod 4$.

Additionally, it holds $q \notin P$. Suppose the contrary. Then $q=p_j$ for some $1 \le j \le n$. As q is a prime factor of a, it holds $q \mid a$. As $q=p_j$ it holds $p_j \mid 4p_1p_2\dots p_n$. But then it must also hold that $q \mid (-1)$. However, this is impossible as only for $q=1, a=-1$ and $q=-1, a=1$ the divisbility definition $qa=-1$ is fulfilled. However, q is primes and primes are defined to be strictly greater than 1. This contradiction concludes the proof that $q \notin P$.

So in the end we have $q \equiv 3 \mod 4$ and $q \notin P$. This contradicts our initial assumption. Hence, there are infinitely many solutions of the equation $p \equiv 3 \mod 4$.

https://math.stackexchange.com/a/714048
https://math.stackexchange.com/a/1433518
https://math.stackexchange.com/a/30579
pdf from some university