

Solutions to Homework 7, Math 310

(1) Prove the formula,

$$|\cup_{i=1}^n S_i| = \sum_{i=1}^n |S_i| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| - \cdots + (-1)^{n-1} |\cap_{i=1}^n S_i|.$$

(Hint: When notation as above seems confusing, always write out the expressions fully (without summation signs) for small values of n , till it is clear what is meant.)

Proof. Let us write this down for small values of n . For $n = 1$, we just get $|S_1| = |S_1|$. For $n = 2$, we get

$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|.$$

For $n = 3$, we get,

$$|S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|.$$

We use induction to prove the result. So, let $P(n)$ be the statement that given finite sets S_1, \dots, S_n , the above formula holds. Then as we saw, $P(1)$ is just the formula $|S_1| = |S_1|$, which is obvious.

Next we wish to show that $P(n) \Rightarrow P(n+1)$. Put, $\cup_{i=1}^n S_i = T$. Then by $P(n)$ we have the formula above for $|T|$. We have $\cup_{i=1}^{n+1} S_i = T \cup S_{n+1}$. Thus, from class, we have,

$$|\cup_{i=1}^{n+1} S_i| = |T \cup S_{n+1}| = |T| + |S_{n+1}| - |T \cap S_{n+1}|.$$

By distributivity,

$$T \cap S_{n+1} = (\cup_{i=1}^n S_i) \cap S_{n+1} = \cup_{i=1}^n (S_i \cap S_{n+1}).$$

Since there are n finite sets $S_i \cap S_{n+1}$ in this, we may use the fact that $P(n)$ is true to assert that,

$$|T \cap S_{n+1}| = \sum_{i=1}^n |S_i \cap S_{n+1}| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j \cap S_{n+1}| + \cdots$$

Putting all these together, one has,

$$\begin{aligned}
|\cup_{i=1}^{n+1} S_i| &= |T| + |S_{n+1}| - |T \cap S_{n+1}| \\
&= \sum_{i=1}^n |S_i| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| - \dots \\
&\quad + |S_{n+1}| - \sum_{i=1}^n |S_i \cap S_{n+1}| + \sum_{1 \leq i < j \leq n} |S_i \cap S_j \cap S_{n+1}| - \dots \\
&= \sum_{i=1}^{n+1} |S_i| - \sum_{1 \leq i < j \leq n+1} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n+1} |S_i \cap S_j \cap S_k| - \dots
\end{aligned}$$

This is just the statement $P(n+1)$, which proves the result by induction. □

(2) Recall the definition of a prime number.

Definition 1. An element $p \in \mathbb{N}$ is a prime number if $p > 1$ and if $a \in \mathbb{N}$ divides p , then $a = 1$ or $a = p$.

(a) If $p \in \mathbb{N}$ is a prime number and $a, b \in \mathbb{N}$ with p dividing ab , show that p divides a or p divides b . (Hint: Use properties of gcd done in an earlier homework).

Proof. If we let $\gcd(p, a) = d$ then d must divide p and by definition of prime, we see that $d = 1$ or $d = p$. If $d = p$, then since d also divides a by definition of gcd, we see that p divides a , which proves the result we set out to prove. So, assume that $\gcd(a, p) = 1$.

From the properties of gcd, we can write $1 = \alpha p + \beta a$ for some integers α, β . Multiplying this equation by b , we get $b = \alpha p b + \beta a b$. But, p divides the first term in an obvious manner and it divides the second term since $p \mid ab$ by assumption. So, p divides b . □

(b) Show that any $n \in \mathbb{N}$, $n > 1$ can be written uniquely as a product of primes. That is, given such an n , there exists prime numbers p_1, p_2, \dots, p_m for some $m \in \mathbb{N}$ so that $n = p_1 p_2 \cdots p_m$ and this expression is unique upto reordering the p_i s. (Hint: Use the version of induction $(P(n))(\forall n \leq N) \Rightarrow P(N+1)$).

Proof. Let $P(N)$ for $N \geq 2$ be the predicate that N can be written as a product of primes. Then $P(2)$ is true. Next we will show that $(P(n))(2 \leq n \leq N) \Rightarrow P(N + 1)$ and then one easily sees by this version of induction, that $P(N)$ is true for all $N \geq 2$. This will prove the result. We will deal with the uniqueness later.

So, assume $(P(n))(2 \leq n \leq N)$. If $N + 1$ is a prime, clearly $N + 1$ can be written as just $N + 1$, product of one prime and thus $P(N + 1)$ is true. If not, $N + 1$ is not a prime and thus by definition, there exists an $a \in \mathbb{N}$ which divides $N + 1$ and $1 \neq a \neq N + 1$. Writing $N + 1 = ab$ with $b \in \mathbb{N}$ (which is what division means), since $1 \neq a \neq N + 1$, we see that $1 < a, b < N + 1$. So we have $2 \leq a, b \leq N$ and therefore by our assumption, $P(a)$ and $P(b)$ are true. So, we can write $a = p_1 \cdots p_m$ and $b = q_1 \cdots q_l$ for primes p_i, q_j . Thus $N + 1 = p_1 \cdots p_m \cdot q_1 \cdots q_l$, and so $N + 1$ can be written as a product of primes, proving $P(N + 1)$. So, by induction, we are done.

Lastly to show uniqueness, we proceed as follows by induction. Let $P(r)$ be the predicate that if a number $n \in \mathbb{N}$, $n \geq 2$ can be written as a product of r primes, then the expression is unique upto reordering. From the previous part, if we prove that $P(r)$ is true for all $r \in \mathbb{N}$, we would be done, since we have shown that any natural number $n \geq 2$ can be written as a finite product of primes at least in one way.

We first check that $P(1)$ is true. If n can be written as a product of just one prime, it just means that n is a prime. If it has another expression, write $n = q_1 \cdots q_l$. Then q_1 divides n and by definition of a prime, $q_1 = n$. But then it is clear that $q_i, i > 1$ must be all 1 and so can not be primes. Thus $n = q_1$ is the only possible expression.

Next we check that $P(r) \Rightarrow P(r + 1)$. So, let

$$(1) \quad n = p_1 \cdots p_{r+1} = q_1 \cdots q_l \quad \text{for primes } p_i, q_j.$$

So, p_{r+1} divides $q_1 \cdots q_l$ and from the previous problem, it is easy to see that then p_{r+1} must divide one of the q_i s, which after reordering, we may assume is q_l . But, p_{r+1}, q_l are primes and $p_{r+1} \mid q_l$ implies $p_{r+1} = q_l$ by definition of prime. Cancelling these in equation 1, we get $p_1 \cdots p_r = q_1 \cdots q_{l-1}$. But, since $P(r)$ is true, this means $l - 1 = r$

and $p_i = q_j$ after reordering. Thus the original expression also must have been unique, proving $P(r + 1)$. \square

- (3) Let $f : A \rightarrow A$ be a function. Define f^n to be composite $f \circ f \circ \dots \circ f$, n times. For example, $f^2 = f \circ f$ and $f^3 = f \circ f \circ f$. Show that if $f^n = \text{Id}_A$, then f is bijective.

Proof. If $n = 1$, there is nothing to prove, since then $f = \text{Id}_A$. So, assume that $n \geq 2$. Let $g = f^{n-1}$. Then $f \circ g = f^n = \text{Id}_A$ and $g \circ f = f^n = \text{Id}_A$. So, f has an inverse, namely g and from what we proved in class, f is bijective. \square

- (4) Construct functions $f_n : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ for any natural number $n \geq 2$ so that $f_n^n = \text{Id}_{\mathbb{R}^2}$, but $f_n^m \neq \text{Id}_{\mathbb{R}^2}$ for $1 \leq m < n$.

Proof. Any element in \mathbb{R}^2 can be written in polar coordinates as $t = (r \cos \theta, r \sin \theta)$ for a real number $r \geq 0$ and $\theta \in \mathbb{R}$. Define

$$f_n(t) = (r \cos(\theta + \frac{2\pi}{n}), r \sin(\theta + \frac{2\pi}{n})).$$

I will leave you to check that f_n has the properties stated. Notice that the function is just a counterclockwise rotation around the origin by an angle $\frac{2\pi}{n}$. \square

- (5) If A, B are finite sets with $|A| = m \geq 1$ and $|B| = n \geq 1$, show that the set of all functions from $A \rightarrow B$, denoted by $\text{Fun}(A, B)$ is a finite set and $|\text{Fun}(A, B)| = n^m$.

Proof. We use induction on m . So, let the predicate $P(m)$ be that if B is a finite set with $|B| = n \geq 1$ and A is a finite set with $|A| = m$, then $\text{Fun}(A, B)$ is a finite set and $|\text{Fun}(A, B)| = n^m$. Notice that the predicate depends on m and not on n . That is, n is kept fixed and we let m vary.

As usual, we check $P(1)$ is true. So, let A be a set with one element. Then any function $f : A \rightarrow B$ is completely determined by where this element goes and it has n choices, from elements of B . Thus the set of all these functions is finite and its cardinality is $n = n^1$.

Now, let us check that $P(m) \Rightarrow P(m + 1)$. So, let A be a set with $m + 1$ elements and let $a \in A$. Let $C = A \setminus \{a\}$. So, $|C| = m$ and thus by induction hypothesis, $\text{Fun}(C, B)$ is a finite set and

$$(2) \quad |\text{Fun}(C, B)| = n^m.$$

Next we define a function $F : \text{Fun}(A, B) \rightarrow \text{Fun}(C, B) \times B$ as follows. If $f \in \text{Fun}(A, B)$, then $F(f) = (f|_C, f(a))$, where

$f|_C : C \rightarrow B$ is the function defined as $f|_C(x) = f(x)$ for any $x \in C$. We will show that F is bijective.

As usual, we first show that it is injective and then surjective. To show injectivity, let $f, g \in \text{Fun}(A, B)$ and assume that $F(f) = F(g)$. We wish to show that $f = g$. So, we must show that $f(x) = g(x)$ for all $x \in A$. Our assumption $F(f) = F(g)$ means $f|_C = g|_C$ and $f(a) = g(a)$. If $a \neq x \in A$, then $x \in C$ and thus $f(x) = f|_C(x) = g|_C(x) = g(x)$. Since $f(a) = g(a)$, we see that $f(x) = g(x)$ for all $x \in A$ and thus $f = g$, proving injectivity.

Next we check surjectivity. So, let $(p, b) \in \text{Fun}(C, B) \times B$. Define a function $f : A \rightarrow B$ as follows. $f(x) = p(x)$ if $x \in C$ and $f(a) = b$. Since $A = C \cup \{a\}$, we have defined a function. Since $f|_C = p$ and $b = f(a)$, we see that $F(f) = (p, b)$, proving surjectivity.

By equation 2 and what we have seen in class, $\text{Fun}(C, B) \times B$ is a finite set and its cardinality is $n^m \times n = n^{m+1}$. Since F is bijective, we see that $\text{Fun}(A, B)$ is a finite set and its cardinality is n^{m+1} . This proves $P(m+1)$ and thus by induction, we are done.

□

- (6) Let $\mathbb{R}[x]$ denote the set of all polynomials. Show that the function $d : \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ given by $d(f(x)) = \frac{df(x)}{dx}$ is surjective but not injective.

Proof. Clearly the constant polynomial, say 1, is in $\mathbb{R}[x]$ and it goes to zero under differentiation. Of course so does the zero polynomial, and hence the map is not injective.

Given a polynomial $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, take

$$g(x) = a_0 \frac{x^{n+1}}{n+1} + a_1 \frac{x^n}{n} + \cdots + a_n x.$$

Then, $d(g(x)) = f(x)$, proving surjectivity.

□