HOMEWORK 5

LEANDRO RIBEIRO
(WORKED WITH KYLE FRANKE AND JOYCE GOMEZ)

Proposition 4.32. *For all k,m* $\in \mathbb{N}$*,* f_{mk} *is divisible* f_m*.*

Proof. Let P(k) be the statement "f_{mk} is divisible f_m." Let's first observe P(1).
Base. k = 1. $f_{m(1)} = f_m = f_m \cdot 1$.
Successor. Assume P(k). That is, f_{mk} is divisible f_m. Consider $f_{m(k+1)}$. $f_{m(k+1)} = f_{mk+m}$. By proposition 4.30, we can rewrite this as $f_{mk}f_{m-1} + f_{mk+1}f_m$. By induction, we have that $f_{mk} = f_m j$ for some j $\in \mathbb{Z}$. Hence, $f_m j f_{m-1} + f_{mk+1}f_m = f_m(jf_{m-1} + f_{mk+1})$. We have proven P(k+1), and thus proven the proposition by induction. □

Project 5.16. *Someone tells you that the following equalities are true for all sets A,B,C. In each case, either prove the claim or provide a counterexample.*
(i) $A - (B \cup C) = (A - B) \cup (A - C)$.
(ii) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

(i) Say A = {1,2,3,4}, B = {3,4,5}, and C = {1,6,7}. $A - (B \cup C) = \{2\}$. On the other hand, $(A - B) \cup (A - C) = \{1, 2, 3, 4\}$. Thus, the claim does not hold

Proof. (ii) $A \cap (B - C)$ is the intersection between A and B not including the elements in B that are also in C. Suppose we have an x $\in A \cap (B - C)$, by definition of intersection, we know x $\in A$ and x $\in (B - C)$. If x $\in (B - C)$, by definition, x $\in B$ but x $\notin C$. Because x $\in A$, x $\in B$, and x $\notin C$, $x \in (A \cap B)$ and x $\notin (A \cap C)$. By definition of set subtraction, x $\in (A \cap B) - (A \cap C)$. Thus, $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$.

Now assume x $\in (A \cap B) - (A \cap C)$. By definition, this means x$\in (A \cap B)$ and x $\notin (A \cap C)$. Because x $\in (A \cap B)$, this means x $\in A$ and x $\in B$ by definition of intersection. Because x $\in A$ but x $\notin (A \cap C)$, this means x $\notin C$. Because x $\in B$ but x $\notin C$, x $\in (B - C)$ by definition of set subtraction. Since we already know x $\in A$ and x $\in (B - C)$, we can conclude x $\in A \cap (B - C)$ by definition of intersection. Hence, $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$. Since $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$

Date: February 20, 2017.

and $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$, we may conclude $A \cap (B - C) = (A \cap B) - (A \cap C)$. □

Proposition 5.20. *Let A,B,C be sets.*
(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
(ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. (i) Let x $\in A \times (B \cup C)$. By definition, this means x = (y,z) where y $\in A$ and z $\in (B \cup C)$. By definition of union, this means z $\in B$ or z $\in C$.
Case 1: z $\in B$. Since y $\in A$ and z $\in B$, x $\in (A \times B)$. Thus by definition of union x $\in (A \times B) \cup (A \times C)$.
Case 2: z $\in C$. Since y $\in A$ and z $\in C$, x $\in (A \times C)$. Thus by definition of union x $\in (A \times B) \cup (A \times C)$.

We've proven that in both cases x $\in (A \times B) \cup (A \times C)$. Therefore, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Now let x $\in (A \times B) \cup (A \times C)$. This means x $\in (A \times B)$ or x $\in (A \times C)$.
Case 1: x $\in (A \times B)$. This means x = (y,z) where y $\in A$ and z $\in B$. By definition of union, because z $\in B$, z $\in (B \cup C)$. Because y $\in A$ and z $\in (B \cup C)$, x $\in A \times (B \cup C)$ By definition of $\times$.
Case 2: x $\in (A \times C)$. This means x = (y,z) where y $\in A$ and z $\in C$. By definition of union, because z $\in C$, z $\in (B \cup C)$. Because y $\in A$ and z $\in (B \cup C)$, x $\in A \times (B \cup C)$ By definition of $\times$.

We've proven that in both cases x $\in A \times (B \cup C)$. Therefore, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. Because $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$ and $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, $A \times (B \cup C) = (A \times B) \cup (A \times C)$ by mutual inclusion.

□

Proposition 6.6. *(i) Given an equivalence relation on A, its equivalence classes form a partition of A.*

(ii) Conversely, given a partition Π *of A, define* $\sim$ *by* $a \sim b$ *if and only if a and b lie in the same element of* Π*. Then* $\sim$ *is an equivalence relation.*

Proof. (i) Set $\Pi = \{[a] | a \in A\}$. Let's first argue every a $\in A$ is in some member of Π. Clearly [a] $\in \Pi$ and by proposition 6.4, a $\in [a]$. Hence every a $\in A$ lies in some $P \in \Pi$. By 6.5 for any [a], [b] $\in \Pi$ either [a] = [b] or $[a] \cap [b] = \emptyset$. If [a] $\neq$ [b], then [a] $\cap$ [b] = $\emptyset$, by 6.5. Thus Π is a partition.
(ii) We define $a \sim b$ if and only if a,b $\in P \in \Pi$. **Reflexivity:** Since a is in the same part of the partition as itself, $a \sim a$. **Symmetry:** If a

and b are in the same part $P \in \Pi$, then b and a are in the same part. Hence $a \sim b$ if and only if $b \sim a$. **Transitivity:** If a and b are in the same part $P \in \Pi$, and if b and c are in the same part $P \in \Pi$, then a and c are in the same part. Thus, $a \sim c$. □

Proposition 6.18. ***(Division Algorithm for Polynomials).*** *Let n(x) be a polynomial that is not zero. For every polynomial m(x), there exist polynomials q(x) and r(x) such that*

m(x) = q(x)n(x) + r(x)

and either r(x) is zero or the degree of r(x) is smaller than the degree of n(x).

Proof. By definition, $m(x) = a_d x^d + \cdots + a_0$. Let P(d) be the statement "m(x) = q(x)n(x) + r(x)." Let's first observe P(0).
Base. d = 0. This means $m(x) = a_0$. a_0 is a constant, so by proposition 6.13 (the division algorithm) we know that $a_0 = qn + r$ for constants $q(x) = q, n(x) = n$, and $r(x) = r$.
Successor. Assume P(n) holds. That is, $m(x) = a_n x^n + \cdots + a_0 = q(x)n(x) + r(x)$. Consider $m(x) = a_{n+1}x^{n+1} + \cdots + a_0$. I'm unsure what to do from this point on. But we must apply induction to prove P(n+1) holds. □

Proposition 6.25. *If $a \equiv a'$ (mod n) and $b \equiv b'$ (mod n) then $a + b \equiv a' + b'$ (mod n) and $ab \equiv a'b'$ (mod n).*

Proof. By definition, $a \equiv a'$ (mod n) means a - a' = qn, and $b \equiv b'$ (mod n) means b - b' = rn for some q,r $\in \mathbb{Z}$. If we add these equations together, we have a - a' + b - b' = qn + rn. We can rewrite this as (a + b) - (a' + b') = (q + r)n. By definition of ≡, a + b ≡ a' + b' (mod n).

Consider ab - a'b'. Adding and subtracting ab', we have ab + ab' - ab' -a'b' = a(b - b') + (a - a')b'. Substituting, we have a(rn) + (qn)b'. This is equal to n(ar +qb'). Since, the expression is divisible by n, we can conclude ab ≡ a'b' (mod n). □

Sources.
http://zimmer.csufresno.edu/ sdelcroix/sol111home6.pdf
http://zimmer.csufresno.edu/ sdelcroix/sol111home8.pdf