MTH302: *Set Theory and Mathematical Logic*
Homework: These will be periodically updated. Odd Semester, 2021/22

(1) Show that there is no set V such that every set is a member of V.

Solution: Suppose not and let V be a set such that every set is a member of V. Define $W = \{x \in V : x \notin x\}$. Then W is a set by the axiom of comprehension. Since W is a set, either $W \in W$ or $W \notin W$. If $W \in W$, then since $W \in V$, we must have $W \notin W$. Similarly, if $W \notin W$, then $W \in W$. In either case we get a contradiction. Hence V does not exist. $\square$

(2) Show that $(x, y) = (a, b)$ iff $x = a$ and $y = b$.

Solution: The right to left implication is obvious. So assume $(x, y) = (a, b)$ and we'll show $x = a$ and $y = b$. We consider two cases.

Case $x = y$: In this case, $(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}\}$. Hence $(a, b) = \{\{a\}, \{a, b\}\} = \{\{x\}\}$. It follows that $\{x\} = \{a\} = \{a, b\}$. So $x = a = b$. Hence $x = y = a = b$.

Case $x \neq y$: In this case, $\{\{x\}, \{x, y\}\}$ is a set with two distinct members. It follows that $\{\{a\}, \{a, b\}\}$ is also a set with two distinct members. So $a \neq b$. Now $\{x\} \in \{\{a\}, \{a, b\}\}$ implies $\{x\} = \{a\}$ since $\{x\} \neq \{a, b\}$ (as the latter has two distinct members). Similarly, $\{x, y\} = \{a, b\}$. As $x = a$, and $y \neq x$, we get $y = b$. $\square$

(3) Suppose R is an equivalence relation on A. For each $a \in A$, define the R-equivalence class of a by $[a] = \{b \in A : aRb\}$. Show that $\{[a] : a \in A\}$ is a partition of A. Furthermore, show that for every partition $\mathcal{F}$ of A, there is an equivalence relation S on A such that $\mathcal{F}$ is the set of all S-equivalence classes.

Solution: To show that $\{[a] : a \in A\}$ is a partition of A, we need to show that $\bigcup\{[a] : a \in A\} = A$ and for any two distinct R-equivalence classes $[a], [b]$, we must have $[a] \cap [b] = \emptyset$.

Since R is a reflexive relation on A, for every $a \in A$, $a \in [a]$. Hence $A \subseteq \bigcup\{[a] : a \in A\}$. As $[a] \subseteq A$ for every $a \in A$, we also have $\bigcup\{[a] : a \in A\} \subseteq A$. Thus $\bigcup\{[a] : a \in A\} = A$.

Next, towards a contradiction, suppose $a, b \in A$, $[a] \neq [b]$ and $[a] \cap [b] \neq \emptyset$. Fix $c \in [a] \cap [b]$. Since $c \in [a]$, we get aRc. Similarly, bRc. Since R is symmetric, it follows that cRb. Since aRc and cRb, using the fact that R is transitive, we get aRb and hence also bRa (as R is symmetric). We now claim the following.

$[a] \subseteq [b]$: Fix $x \in [a]$. Then aRx. As bRa, by transitivity of R, we get bRx. Hence $x \in [b]$. So $[a] \subseteq [b]$.

$[b] \subseteq [a]$: Fix $y \in [b]$. Then bRy. As aRb, by transitivity of R, we get aRy. Hence $y \in [a]$. So $[b] \subseteq [a]$.

It follows that $[a] = [b]$ which contradicts our assumption that $[a] \neq [b]$. This finishes the proof that $\{[a] : a \in A\}$ is a partition of A.

Now fix a partition $\mathcal{F}$ of A and define a relation S on A as follows. For $a, b \in A$, aSb iff there exists $E \in \mathcal{F}$ such that both a and b are members of E.

Let us first check that S is an equivalence relation on A. It is clear that S is a symmetric relation on A. Since $\bigcup \mathcal{F} = A$, it follows that S is reflexive. Next suppose aSb and bSc. Fix E, F in $\mathcal{F}$ such that $a, b \in E$ and $b, c \in F$. Since $\mathcal{F}$ has pairwise disjoint members and since $E \cap F \neq \emptyset$, we must have $E = F$. Hence aSc. So S is transitive. It follows that S is an equivalence relation on A.

Finally, let us check that the set $\{[a] : a \in A\}$ of S-equivalence classes is equal to $\mathcal{F}$. Let $[a]$ be an S-equivalence class. Fix $E \in \mathcal{F}$ such that $a \in E$. Then by the definition of S, it follows that $[a] = \{b \in A : aSb\} = \{b \in A : b \in E\} = E$. Conversely, if $E \in \mathcal{F}$, then for every $a \in E$, $[a] = E$. Hence $\{[a] : a \in A\} = \mathcal{F}$. $\square$

(4) Let $(L, \prec)$ be a linear ordering. Prove the following.

(a) $(L, \prec)$ is a well-ordering iff there is no sequence $\langle x_n : n < \omega \rangle$ in L such that $(\forall n < \omega)(x_{n+1} \prec x_n)$.

(b) $(L, \prec)$ is a well-ordering iff for every $A \subseteq L$, $(A, \prec)$ is isomorphic to an initial segment of $(L, \prec)$.

Solution: (a) First suppose that $(L, \prec)$ is a well-ordering. We'll show that there is no $\prec$-decreasing sequence in L. Towards a contradiction, suppose there is a sequence $\langle x_n : n < \omega \rangle$ in L such that for every $n < \omega$, $x_{n+1} \prec x_n$. Let $A = \{x_n : n < \omega\}$ be the range of this sequence. Then A has no $\prec$-least member which contradicts the fact that $(L, \prec)$ is a well-ordering.

Now suppose $(L, \prec)$ is not a well-ordering and fix a nonempty $A \subseteq L$ such that A does not have a $\prec$-least member. We'll construct a $\prec$-decreasing sequence $\langle x_n : n < \omega \rangle$ in L. Using the axiom of choice, fix a choice function $F : \mathcal{P}(A) \setminus \{\emptyset\} \to A$. So for every nonempty $W \subseteq A$, $F(W) \in W$. By recursion on $n < \omega$, define $\langle x_n : n < \omega \rangle$ as follows. $x_0 = F(A)$ and for every $n < \omega$,

$$x_{n+1} = F\left(\{x \in A : x \prec x_n\}\right)$$

Note that this is well-defined since $\{x \in A : x \prec a_n\}$ is nonempty (as A has no $\prec$-least member). It is clear that $\langle x_n : n < \omega \rangle$ is as required. $\square$

(b) First suppose $(L, \prec)$ is a well-ordering. Fix $A \subseteq L$. We'll construct an isomorphism from $(A, \prec)$ to an initial segment of $(L, \prec)$. Define

$$f = \{(x, a) \in L \times A : (\mathsf{pred}(L, \prec, x), \prec) \cong (\mathsf{pred}(A, \prec, a), \prec)\}$$

(i) f $\mathsf{is\ a\ function}$: Clearly, f is a relation. To see that it is a function, fix $(x, a), (x, b) \in f$ and we'll show that $a = b$. Towards a contradiction suppose $a \neq b$. Without loss of generality suppose $a \prec b$. Since (x, a) and (x, b) are both in f, we get $(\mathsf{pred}(L, \prec, x), \prec) \cong (\mathsf{pred}(A, \prec, a), \prec)$ and $(\mathsf{pred}(L, \prec, x), \prec) \cong (\mathsf{pred}(A, \prec, b), \prec)$.

Hence $(\mathsf{pred}(A, \prec, a), \prec) \cong (\mathsf{pred}(A, \prec, b), \prec)$. But this means that $(\mathsf{pred}(A, \prec, b), \prec)$ is a well-ordering that is isomorphic to a proper initial segment of itself. Contradiction. So f is a function.

(ii) f is injective: The proof is similar to (i) above.

(iii) $\mathrm{dom}(f)$ is an initial segment of $(L, \prec)$: Suppose $x \in \mathrm{dom}(f)$ and $y \prec x$. We need to show that $y \in \mathrm{dom}(L)$. Let $f(x) = a$. Fix an isomorphism $h : (\mathsf{pred}(L, \prec, x), \prec) \to (\mathsf{pred}(A, \prec, a), \prec)$. Note that $y \in \mathrm{dom}(h)$. Let $h(y) = b$. It is clear that $h \restriction \mathsf{pred}(L, \prec, y)$ is an isomorphism from $(\mathsf{pred}(L, \prec, y), \prec)$ to $(\mathsf{pred}(A, \prec, b), \prec)$. Hence $(y, b) \in f$ and so $y \in \mathrm{dom}(f)$.

(iv) $\mathrm{range}(f)$ is an initial segment of $(A, \prec)$: The proof is similar to (iii) above.

(v) f is an isomorphism from $(\mathrm{dom}(f), \prec)$ to $(\mathrm{range}(f), \prec)$: Suppose $x \prec y$ are in $\mathrm{dom}(f)$. Put $a = f(x)$ and $b = f(y)$. Using the definition of f, it follows that $(\mathsf{pred}(L, \prec, x), \prec) \cong (\mathsf{pred}(A, \prec, a), \prec)$ and $(\mathsf{pred}(L, \prec, y), \prec) \cong (\mathsf{pred}(A, \prec, b), \prec)$. As $x \prec y$, it follows that $(\mathsf{pred}(A, \prec, a), \prec)$ is isomorphic to an initial segment of $(\mathsf{pred}(A, \prec, b), \prec)$. Since no well-ordering can be isomorphic to a proper initial-segment of itself, it follows that $a \prec b$. So f is an isomorphism from $(\mathrm{dom}(f), \prec)$ to $(\mathrm{range}(f), \prec)$.

(vi) $\mathrm{range}(f) = A$: Suppose not. Let $a = \min(A \setminus \mathrm{range}(f))$. Since $\mathrm{range}(f)$ is an initial segment of $(A, \prec)$, it follows that $\mathrm{range}(f) = \mathsf{pred}(A, \prec, a)$. We claim that $\mathrm{dom}(f) = L$. For suppose not and let $x = \min(L \setminus \mathrm{dom}(f))$. Then $\mathrm{dom}(f) = \mathsf{pred}(L, \prec, x)$. But this implies that $(a, b) \in f$ using (i)-(v) above which is a contradiction. So $\mathrm{dom}(f) = L$. Hence $a \in \mathrm{dom}(f)$. Now observe that $f(a) \prec a$ (since $\mathrm{range}(f) = \mathsf{pred}(A, \prec, a)$) and iteratively applying f, we get $a \succ f(a) \succ f(f(a)) \succ \dots$. But this means that $(L, \prec)$ has an infinite $\prec$-descending sequence which is impossible by part (a).

(i)-(vi) imply that $(A, \prec)$ is isomorphic (via f^{-1}) to an initial segment of $(L, \prec)$ (namely $\mathrm{dom}(f)$).

Next we show the converse. Suppose for every $A \subseteq L$, $(A, \prec)$ is isomorphic to an initial segment of $(L, \prec)$. We'll show that $(L, \prec)$ must be a well-ordering. We can assume that $L \neq \emptyset$. Let $a \in L$. Then $(\{a\}, \prec)$ is isomorphic to an initial segment f $(L, \prec)$. This implies that L has a $\prec$-least element, say x. Now let $A \subseteq L$ be nonempty and fix an isomorphism $f : (A, \prec) \to (W, \prec)$ where W is an initial segment of $(L, \prec)$. Note that $x \in W$. Put $a = f^{-1}(x)$. Then a is the $\prec$-least element of A. It follows that $(L, \prec)$ is a well-ordering. $\square$

(5) Suppose $(X, \prec_1)$ and $(Y, \prec_2)$ are well-orderings. Then exactly one of the following holds.

   (a) $(X, \prec_1) \cong (Y, \prec_2)$.

   (b) For some $x \in X$, $(\mathsf{pred}(X, \prec_1, x), \prec_1) \cong (Y, \prec_2)$.

   (c) For some $y \in Y$, $(\mathsf{pred}(Y, \prec_2, y), \prec_2) \cong (X, \prec_1)$.

Furthermore, in each of the three cases, the isomorphism is unique.

Solution: Define

$$f = \{(a, b) \in X \times Y : (\mathsf{pred}(X, \prec_1, a), \prec_1) \cong (\mathsf{pred}(Y, \prec_2, b), \prec_2)\}$$

(i) f is a function: Clearly, f is a relation. To see that it is a function, fix $(a, b), (a, c) \in f$ and we'll show that $b = c$. Towards a contradiction suppose $b \neq c$. Without loss of generality suppose $b \prec_2 c$. Since (a, b) and (a, c) are both in f, we get $(\mathsf{pred}(X, \prec_1, a), \prec_1) \cong (\mathsf{pred}(Y, \prec_2, b), \prec_2)$ and $(\mathsf{pred}(X, \prec_1, a), \prec_1) \cong (\mathsf{pred}(Y, \prec_2, c), \prec_2)$. Hence $(\mathsf{pred}(Y, \prec_2, c), \prec_2) \cong (\mathsf{pred}(Y, \prec_2, b), \prec_2)$. But this means that $(\mathsf{pred}(Y, \prec_2, c), \prec_2)$ is a well-ordering that is isomorphic to a proper initial segment of itself. Contradiction. So f is a function.

(ii) f is injective: The proof is similar to (i) above.

(iii) $\mathsf{dom}(f)$ is an initial segment of $(X, \prec_1)$: Suppose $x \in \mathrm{dom}(f)$ and $y \prec_1 x$. We need to show that $y \in \mathrm{dom}(X)$. Let $f(x) = a$. Fix an isomorphism $h : (\mathsf{pred}(X, \prec_1, x), \prec_1) \to (\mathsf{pred}(Y, \prec_2, a), \prec_2)$. Note that $y \in \mathrm{dom}(h)$. Let $h(y) = b$. It is clear that $h \restriction \mathsf{pred}(X, \prec_1, y)$ is an isomorphism from $(\mathsf{pred}(X, \prec_1, y), \prec_1)$ to $(\mathsf{pred}(Y, \prec_2, b), \prec_2)$. Hence $(y, b) \in f$ and so $y \in \mathrm{dom}(f)$.

(iv) $\mathsf{range}(f)$ is an initial segment of $(A, \prec)$: The proof is similar to (iii) above.

(v) f is an isomorphism from $(\mathsf{dom}(f), \prec_1)$ to $(\mathsf{range}(f), \prec_2)$: Suppose $x \prec_1 y$ are in $\mathrm{dom}(f)$. Put $a = f(x)$ and $b = f(y)$. Using the definition of f, it follows that $(\mathsf{pred}(X, \prec_1, x), \prec_1) \cong (\mathsf{pred}(Y, \prec_2, a), \prec_2)$ and $(\mathsf{pred}(X, \prec_1, y), \prec_1) \cong (\mathsf{pred}(Y, \prec_2, b), \prec_2)$. As $x \prec_1 y$, it follows that $(\mathsf{pred}(Y, \prec_2, a), \prec_2)$ is isomorphic to an initial segment of $(\mathsf{pred}(Y, \prec_2, b), \prec_2)$. Since no well-ordering can be isomorphic to a proper initial-segment of itself, we must have $a \prec_2 b$. So f is an isomorphism from $(\mathrm{dom}(f), \prec_1)$ to $(\mathrm{range}(f), \prec_2)$.

(vi) Either $\mathsf{dom}(f) = X$ or $\mathsf{range}(f) = A$: Suppose not. Let x be the $\prec_1$-least member of $X \setminus \mathrm{dom}(f)$ and let a be the $\prec_2$-least member of $Y \setminus \mathrm{range}(f)$. Since $\mathrm{range}(f)$ is an initial segment of $(Y, \prec_2)$, it follows that $\mathrm{range}(f) = \mathsf{pred}(Y, \prec_2, a)$. Similarly, $\mathrm{dom}(f) = \mathsf{pred}(X, \prec_1, x)$. But now $(x, a) \in f$ using (i)-(v) above which is a contradiction.

If $\mathrm{dom}(f) = X$ and $\mathrm{range}(f) = Y$, we get clause (a). If $\mathrm{dom}(f) \neq X$ and $\mathrm{range}(f) = Y$, we get clause (b). If $\mathrm{dom}(f) = X$ and $rng(f) \neq Y$, we get clause (c).

The uniqueness part follows from the fact that the only isomorphism from a well-ordering to itself is the identity function. $\square$

(6) Let $f : \mathcal{P}(\omega) \setminus \{\emptyset\} \to \omega$ be defined by $f(X) = \min(X)$. Call a well-orderings $(A, \prec)$ f-directed iff $A \subseteq \omega$ and for every $x \in A$,

$$f(\omega \setminus \mathsf{pred}(A, \prec, x)) = x$$

Describe all f-directed well-orderings.

Solution: It is clear that each well-ordering in $\{(\alpha, <) : \alpha \leq \omega\}$ is f-directed. Let us show that there is no other f-directed well-ordering. Suppose $(A, \prec)$ is an f-directed well-ordering. First suppose that A is finite (and nonempty) and let $x_0 \prec x_1 \prec \cdots \prec x_n$ list the members of A where $n < \omega$. Then an easy induction on $k \leq n$ shows that $x_k = k$. Next suppose that A is infinite. Let $\mathsf{type}(A, \prec) = \alpha$. So $\alpha \geq \omega$. Let $\langle x_\beta : \beta < \alpha \rangle$ be an order isomorphism from α to $(A, \prec)$. Once again by induction on $n < \omega$, we get $x_n = n$. Since $A \subseteq \omega$, it follows that $\alpha = \omega$ and hence $(A, \prec) = (\omega, <)$. □

(7) Show that if $\alpha < \beta$ are ordinals, then there is a unique ordinal γ such that $\alpha + \gamma = \beta$. (**Hint**: $\gamma = \mathsf{type}(\beta \setminus \alpha, \in)$).

Solution: Following the hint, put $\gamma = \mathsf{type}(\beta \setminus \alpha, \in)$. Note that

$$(\beta, \in) \cong (\alpha, \in) \oplus (\beta \setminus \alpha, \in)$$

Hence

$$\alpha + \gamma = \alpha + \mathsf{type}((\beta \setminus \alpha, \in)) = \mathsf{type}((\alpha, \in) \oplus (\beta \setminus \alpha, \in)) = \beta$$

To see uniqueness, suppose $\alpha + \gamma_1 = \alpha + \gamma_2 = \beta$. We'll show that $\gamma_1 = \gamma_2$. Suppose not and without loss of generality assume $\gamma_1 < \gamma_2$. Then $\gamma_1 + 1 \leq \gamma_2$. Now

$$\beta = \alpha + \gamma_2 \geq \alpha + (\gamma_1 + 1) = (\alpha + \gamma_1) + 1 > \alpha + \gamma_1 = \beta$$

So $\beta > \beta$ which is impossible. □

(8) Suppose α, β, γ are ordinals and $\alpha + \beta = \alpha + \gamma$. Show that $\beta = \gamma$.

Solution: See problem (7). □

(9) Suppose $\alpha \cdot \alpha = \beta \cdot \beta$. Show that $\alpha = \beta$.

Solution: If α or β is 0, then this is clear. So assume $\alpha \geq 1$ and $\beta \geq 1$. Towards a contradiction, suppose $\alpha \neq \beta$ and without loss of generality say $\alpha < \beta$. Then $\alpha + 1 \leq \beta$. Now

$$\beta \cdot \beta \geq \alpha \cdot (\alpha + 1) = (\alpha \cdot \alpha) + \alpha \geq (\alpha \cdot \alpha) + 1 > \alpha \cdot \alpha$$

which contradicts $\alpha \cdot \alpha = \beta \cdot \beta$. □

(10) Show that there is an uncountable chain in $(\mathcal{P}(\omega), \subseteq)$. [**Hint**: Identify ω with the set of rationals $\mathbb{Q}$ and for each real number x, consider $\{r \in \mathbb{Q} : r \leq x\}$].

Solution: Let $\mathbb{Q}^+$ be the set of positive rational numbers and $\mathbb{R}^+$ be the set of positive real numbers. Define $h : \mathbb{Q}^+ \to \omega$ by

$$h\left(\frac{m}{n}\right) = 2^m 3^n$$

where n, m are coprime. Note that h is injective and hence a bijection from $\mathbb{Q}^+$ to range$(h) \subseteq \omega$. For each $x \in \mathbb{R}^+$, let $A_x = \{r \in \mathbb{Q}^+ : r < x\}$. Then $x < y$ implies $A_x \subsetneq A_y$. Hence $\{A_x : x \in \mathbb{R}^+\}$ is an uncountable chain in $(\mathcal{P}(\mathbb{Q}^+), \subseteq)$. It follows that $\{h[A_x] : x \in \mathbb{R}^+\}$ is an uncountable chain in $(\mathcal{P}(\omega), \subseteq)$. $\square$

(11) Call an ordinal α good iff there exists $X \subseteq \mathbb{R}$ such that $(X, <)$ is order isomorphic to α. Show that α is good iff $\alpha < \omega_1$.

Solution: Observe that α is good iff there is an order preserving function from α to $\mathbb{R}$. By transfinite induction on $\alpha < \omega_1$, we'll show that there exists $f : \alpha \to \mathbb{R}$ such that for every $\beta < \gamma < \alpha$, $f(\beta) < f(\gamma)$.

If $\alpha \leq \omega$, this is clear. So let $\omega \leq \alpha < \omega_1$ and for each $\beta < \alpha$, fix an order preserving function $f_\beta : \beta \to \mathbb{R}$. We will construct an order preserving function from α to $\mathbb{R}$. We have the following cases.

α is successor: Suppose $\alpha = \beta + 1$. For each $n < \omega$, let $h_n : (n, n+1) \to \mathbb{R}$ be an order preserving bijection. For example, take

$$h_n(x) = \tan\left(\pi(x - (n + 0.5)\right)$$

Define $f_\alpha : \alpha \to \mathbb{R}$ as follows:

$$f_\alpha(\eta) = \begin{cases} h_0^{-1}(f_\beta(\eta)) & \text{if } \eta < \beta \\ 1 & \text{if } \eta = \beta \end{cases}$$

Note that $f_\alpha \restriction \beta : \beta \to (0, 1)$ is an order preserving function and $f_\alpha(\beta) = 1$. So $f_\alpha : \alpha \to \mathbb{R}$ is order preserving.

α is limit: Since $|\alpha| = \omega$, we can fix a strictly increasing sequence of ordinals $\langle \beta_n : n < \omega \rangle$ such that $\beta_0 = 0$ and $\sup(\{\beta_n : n < \omega\}) = \alpha$. For each $\eta < \alpha$, define

$$f_\alpha(\eta) = h_n^{-1}(f_{\beta_n}(\eta)) \iff \beta_n \leq \eta < \beta_{n+1}$$

Since $h_n^{-1} \circ f_{\beta_n} : \beta_n \to (n, n+1)$ is order preserving, it follows that f_α maps $\{\eta : \beta_n \leq \eta < \beta_{n+1}\}$ into $(n, n+1)$ in an order preserving way. Hence f_α is an order preserving function from $\displaystyle\bigcup_{n<\omega} \{\eta : \beta_n \leq \eta < \beta_{n+1}\} = \alpha$ to $\mathbb{R}$.

Next we show that there is no order preserving function from ω_1 to $\mathbb{R}$. Suppose not and let $f : \omega_1 \to \mathbb{R}$ be order preserving. For each $\alpha < \omega_1$, choose a rational r_α in the interval $(f(\alpha), f(\alpha + 1))$. Since the set of rationals $\mathbb{Q}$ is countable and ω_1 is uncountable, there must exist $\alpha_1 < \alpha_2 < \omega_1$ such that $r_{\alpha_1} = r_{\alpha_2} = r$. Note that

$$\alpha_1 < \alpha_2 \implies \alpha_1 + 1 \leq \alpha_2 \implies f(\alpha_1 + 1) \leq f(\alpha_2)$$

It follows that $(f(\alpha_1), f(\alpha_1 + 1)) \cap (f(\alpha_2), f(\alpha_2 + 1)) = \emptyset$. But this contradicts the fact that r belongs to both of these intervals. $\square$

(12) Let $(P, \preceq_1)$ be a partial ordering. Show that there exists $\preceq_2$ such that $(P, \preceq_2)$ is a linear ordering and $\preceq_2$ extends $\preceq_1$ which means the following:

$$(\forall a, b \in P)(a \preceq_1 b \implies a \preceq_2 b)$$

Solution: Let $\mathcal{F}$ be the family of all relations $\trianglelefteq$ on P such that $(P, \trianglelefteq)$ is a partial ordering and $\preceq_1 \subseteq \trianglelefteq$. $\mathcal{F}$ is nonempty since $\preceq_1 \in \mathcal{F}$.

We claim that every chain (under inclusion) in $\mathcal{F}$ has an upper bound. Let $C \subseteq \mathcal{F}$ be a chain. Put $\preceq = \bigcup C$. It suffices to show that $\preceq$ is in $\mathcal{F}$. It is clear that $\preceq$ is a reflexive relation on P since $\preceq_1 \subseteq \preceq$. Next, suppose $a \preceq b$ and $b \preceq a$. Choose $\trianglelefteq_1, \trianglelefteq_2$ in C such that $a \trianglelefteq_1 b$ and $b \trianglelefteq_2 a$. Since C is a chain, either $\trianglelefteq_1 \subseteq \trianglelefteq_2$ or $\trianglelefteq_2 \subseteq \trianglelefteq_1$. Say $\trianglelefteq_1 \subseteq \trianglelefteq_2$. Then $a \trianglelefteq_2 b$ and $b \trianglelefteq_2 a$. As $\trianglelefteq_2$ is antisymmetric, it follows that $a = b$. Hence $\preceq$ is antisymmetric. A similar argument shows that $\preceq$ is transitive. Hence $(P, \preceq)$ is a partial ordering and $\preceq_1 \subseteq \preceq$. So $\preceq$ is in $\mathcal{F}$.

Using Zorn's lemma, fix a maximal element $\preceq_2$ in $\mathcal{F}$. We claim that for every a, b in P, either $a \preceq_2 b$ or $b \preceq_2 a$. Suppose this fails for some $a \neq b$ in P. Define

$$\trianglelefteq \quad = \quad \preceq_2 \cup \{(x, y) \in P \times P : x \preceq_2 a \text{ and } b \preceq_2 y\}$$

Note that $a \trianglelefteq b$. We'll show that $(P, \trianglelefteq)$ is a partial ordering and hence $\trianglelefteq \in \mathcal{F}$. This suffices as it contradicts the maximality of $\preceq_2$.

It is clear that $\trianglelefteq$ is a reflexive relation on P. Let us check that $\trianglelefteq$ is antisymmetric. Suppose $x \trianglelefteq y$ and $y \trianglelefteq x$. We have the following three cases.

(i) Both (x, y) and (y, x) are in $\preceq_2$: In this case $x = y$ as $\preceq_2$ is antisymmetric.

(ii) Exactly one of (x, y) and (y, x) is in $\preceq_2$: Say $(y, x) \in \preceq_2$ and $(x, y) \notin \preceq_2$ (The other case is similar). Then $x \preceq_2 a$ and $b \preceq_2 y$. Since $\preceq_2$ is transitive and $b \preceq_2 y$, $y \preceq_2 x$ and $x \preceq_2 a$, we get $b \preceq_2 a$ which is impossible. So this case cannot occur.

(iii) Both (x, y) and (y, x) are not in $\preceq_2$: Then $x \preceq_2 a$, $b \preceq_2 y$, $y \preceq_2 a$ and $b \preceq_2 x$. Since $\preceq_2$ is transitive, $b \preceq_2 x$ and $x \preceq_2 a$, we get $a \preceq_2 b$ which is impossible. So this case doesn't occur.

It follows that $\trianglelefteq$ is antisymmetric. Let us check that $\trianglelefteq$ is transitive. Suppose $x \trianglelefteq y$ and $y \trianglelefteq z$. We'll show $x \trianglelefteq z$. Again, we have the following three cases.

(a) Both (x, y) and (y, x) are in $\preceq_2$: In this case $x \preceq_2 y$ as $\preceq_2$ is transitive. Hence also $x \trianglelefteq z$.

(b) Exactly one of (x, y) and (y, z) is in $\preceq_2$: Say $(x, y) \in \preceq_2$ and $(y, z) \notin \preceq_2$ (The other case is similar). Then $y \preceq_2 a$ and $b \preceq_2 z$. Since $\preceq_2$ is transitive, $x \preceq_2 y$ and $y \preceq_2 a$, we get $x \preceq_a$. Hence $x \preceq_2 a$ and $b \preceq_2 z$. It follows that $x \trianglelefteq z$.

(c) Both (x, y) and (y, z) are not in $\preceq_2$: Then $x \preceq_2 a$, $b \preceq_2 y$, $y \preceq_2 a$ and $b \preceq_2 z$. Since $\preceq_2$ is transitive, $b \preceq_2 y$ and $y \preceq_2 a$, we get $b \preceq_2 a$ which is impossible. So this case doesn't occur.

It follows that $\trianglelefteq$ is transitive. Hence $(P, \trianglelefteq)$ is a partial ordering and the proof is complete. $\square$

(13) Suppose $f : \mathbb{R} \to \mathbb{R}$ is additive and $a = f(1)$.

(a) Show that $f(0) = 0$.

(b) Show that for every $x \in \mathbb{R}$, $f(-x) = -f(x)$.

(c) Show that for every $x \in \mathbb{Q}$, $f(x) = ax$.

Solution: (a) Taking $x = y = 0$, we get $f(0 + 0) = f(0) + f(0)$. So $f(0) = 0$.

(b) Taking $y = -x$, we get $f(x + (-x)) = f(x) + f(-x)$. So $f(x) + f(-x) = f(0) = 0$. Hence $f(-x) = -f(x)$.

(c) For each $m, n \geq 1$, $f(m) = f(n(m/n)) = f(m/n + m/n + \cdots + m/n) = nf(m/n)$. So $f(m/n) = f(m)/n$. Next $f(m) = f(1 + 1 + \cdots + 1) = mf(1) = ma$. So $f(m/n) = a(m/n)$. Also $f(-m/n) = -f(m/n) = a(-m/n)$. It follows that for each nonzero $x \in \mathbb{Q}$, $f(x) = ax$. Since $f(0) = 0$, part (c) follows. $\square$

(14) Let $H \subseteq \mathbb{R}$ be a Hamel basis.

(a) Show that every nonzero $x \in \mathbb{R}$ can be uniquely written as

$$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

where $x_1 < x_2 < \cdots < x_n$ are in H and $a_1, a_2, \ldots a_n$ are nonzero rational numbers. Uniqueness means the following: Suppose

$$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n = b_1y_1 + b_2y_2 + \cdots + a_my_m$$

where $x_1 < x_2 < \cdots < x_n$ and $y_1 < y_2 < \cdots < y_m$ are in H and $a_1, \ldots a_n, b_1, \ldots, b_m$ are nonzero rationals. Show that $m = n$ and for every $1 \leq k \leq n$, $x_k = y_k$ and $a_k = b_k$.

(b) Let $f : H \to \mathbb{R}$. Show that there is a unique additive function $g : \mathbb{R} \to \mathbb{R}$ such that $f \subseteq g$.

Solution: (a) First let us check uniqueness: Suppose

$$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n = b_1y_1 + b_2y_2 + \cdots + a_my_m$$

where $x_1 < x_2 < \cdots < x_n$ and $y_1 < y_2 < \cdots < y_m$ are in H and $a_1, \ldots a_n, b_1, \ldots, b_m$ are nonzero rationals. We must show that $m = n$ and for every $1 \leq k \leq n$, $x_k = y_k$ and $a_k = b_k$. Note that

$$(a_1x_1 + a_2x_2 + \cdots + a_nx_n) - (b_1y_1 + b_2y_2 + \cdots + b_my_m) = 0$$

After collecting like terms this boils down to showing the following. If $w_1 < w_2 < \cdots < w_p$ are in H, $c_1, c_2, \ldots c_p$ are rationals and

$$c_1 w_1 + c_2 w_2 + \cdots + c_p w_p = 0$$

then $c_1 = c_2 = \cdots = c_p = 0$. But this is true because H is $\mathbb{Q}$-linearly independent.

Next suppose $x \in \mathbb{R}$ is nonzero. We must show that x is a finite $\mathbb{Q}$-linear combination of members of H. If $x \in H$, then $x = 1 \cdot x$ hence this is clear. So assume $x \notin H$. As H is a maximal $\mathbb{Q}$-linearly independent subset of $\mathbb{R}$, it follows that $H \cup \{x\}$ is not $\mathbb{Q}$-linearly independent. As H is $\mathbb{Q}$-linearly independent, this means that there are $x_1 < x_2 < \cdots < x_n$ in H and nonzero rationals $a_1, a_2, \ldots a_n, b$ such that

$$a_1 x_1 + a_2 x_2 + \ldots a_n x_n + bx = 0$$

Therefore,

$$x = -\frac{a_1}{b} x_1 - \frac{a_2}{b} x_2 - \cdots - \frac{a_n}{b} x_n$$

(b) Define $g(x)$ as follows. If $x = a_1 x_1 + \ldots a_n x_n$ where $x_1 < \cdots < x_n$ are in H and $a_1, \ldots, a_n$ are rationals, then

$$g(x) = a_1 f(x_1) + \cdots + a_n f(x_n)$$

g is well-defined by part (a). That g is additive is clear from its definition. To see uniqueness suppose $g' : \mathbb{R} \to \mathbb{R}$ is another additive extension of f. Then for every $r \in \mathbb{Q}$, $g'(rx) = rg'(x)$. Hence if $x = a_1 x_1 + \ldots a_n x_n$ where $x_1 < \cdots < x_n$ are in H and $a_1, \ldots, a_n$ are rationals, then

$$g'(x) = a_1 g'(x_1) + \cdots + a_n g'(x_n) = a_1 f(x_1) + \cdots + a_n f(x_n) = g(x)$$

So $g' = g$. $\square$

(15) Show that for every $f : \mathbb{R} \to \mathbb{R}$ there are injective functions $g : \mathbb{R} \to \mathbb{R}$ and $h : \mathbb{R} \to \mathbb{R}$ such that $f = g + h$.

Solution: Let $\langle x_\alpha : \alpha < \mathfrak{c} \rangle$ be an injective sequence whose range is $\mathbb{R}$. Using transfinite recursion, construct $\langle y_\alpha : \alpha < \mathfrak{c} \rangle$ as follows.

(1) $y_0 = 0$.

(2) Suppose $1 \leq \alpha < \mathfrak{c}$ and $\langle y_\beta : \beta < \alpha \rangle$ has been defined. Put

$$W = \{y_\beta : \beta < \alpha\} \cup \{y_\beta + f(x_\alpha) - f(x_\beta) : \beta < \alpha\}$$

Then $|W| < \mathfrak{c}$. So choose $y \in \mathbb{R} \setminus W$ and define $y = y_\alpha$. Note that $y_\alpha \notin \{y_\beta : \beta < \alpha\}$ and $f(x_\alpha) - y_\alpha \notin \{f(x_\beta) - y_\beta : \beta < \alpha\}$.

Define $g(x_\alpha) = y_\alpha$ and $h(x_\alpha) = f(x_\alpha) - y_\alpha$ for every $\alpha < \mathfrak{c}$. It is clear that g, h are as required. $\square$

(16) Suppose $f : \mathbb{R} \to \mathbb{R}$ satisfies: For every $x, y \in \mathbb{R}$, $f(x+y) = f(x)f(y)$.

(a) Show that either f is identically zero or range$(f) \subseteq \mathbb{R}^+$.

(b) Suppose f is continuous and not identically zero. Show that $f(x) = a^x$ for some $a > 0$.

Solution: (a) Suppose there is some $a \in \mathbb{R}$ such that $f(a) = 0$. Then for every $x \in \mathbb{R}$, $f(x+a) = f(x)f(a) = f(x) \cdot 0 = 0$. Hence f is identically zero. Next suppose $f(a) \neq 0$ for every $a \in \mathbb{R}$. Then $f(x) = f(x/2 + x/2) = (f(x/2))^2 > 0$. So either f is identically zero or range$(f) \subseteq \mathbb{R}^+$.

(b) By part (a), range$(f) \subseteq \mathbb{R}^+$ so we can define $g(x) = \ln(f(x))$. Then g is a continuous additive function and hence $g(x) = bx$ where $b = g(1)$. It follows that $f(x) = e^{g(x)} = e^{bx} = a^x$ where $a = e^b > 0$. □

(17) Show that there is a discontinuous function $f : \mathbb{R} \to \mathbb{R}$ such that $f(x+y) = f(x)f(y)$ for every $x, y \in \mathbb{R}$.

Solution: Let $g : \mathbb{R} \to \mathbb{R}$ be any discontinuous additive function and define $f(x) = e^{g(x)}$. □

(18) Prove the following.

(a) For every ordinal α, $|\alpha| \leq \alpha$.

(b) If κ is a cardinal and $\alpha < \kappa$, then $|\alpha| < \kappa$.

(c) There is an injection from X to Y iff $|X| \leq |Y|$.

(d) There is a surjection from X to Y iff $|Y| \leq |X|$.

(e) There is a bijection from X to Y iff $|X| = |Y|$.

Solution: Let us write $X \preceq Y$ iff there is an injection from X to Y and $X \sim Y$ iff there is a bijection from X to Y.

(a) Let $|\alpha| = \beta$. Then for every γ, if $\gamma \sim \alpha$, then $\beta \leq \gamma$. Since $\alpha \sim \alpha$, it follows that $\alpha \leq \beta = |\alpha|$.

(b) By part (a), $|\alpha| \leq \alpha < \kappa$.

(c) Since $X \sim |X|$ and $Y \sim |Y|$, we get $X \preceq Y$ iff $|X| \preceq |Y|$. So it suffices to show that if κ, λ are cardinals, then $\kappa \preceq \lambda$ iff $\kappa \leq \lambda$. It is clear that if $\kappa \leq \lambda$, then $\kappa \preceq \lambda$. Next suppose $\lambda < \kappa$. Since $|\kappa| = \kappa$ and $\lambda < \kappa$, $\lambda \nsim \kappa$. Since $\lambda \preceq \kappa$, by the Schröder-Bernstein theorem, it follows that $\kappa \npreceq \lambda$.

(d) By part (c), it suffices to show that for any X and Y, there is a surjection from X to Y iff $Y \preceq X$. We can assume that X, Y are nonempty. Suppose $Y \preceq X$. Fix an injective function $f : Y \to X$. Then $f : Y \to \text{range}(f)$ is a bijection. Fix $y_0 \in Y$. Define $g : X \to Y$ as follows: If $x \in \text{range}(f)$, then $g(x) = f^{-1}(x)$, otherwise $g(x) = y_0$. Clearly, range$(g) = Y$.

Next suppose $f : X \to Y$ and range$(f) = Y$. Let $\mathcal{F} = \{f^{-1}[\{y\}] : y \in Y\}$. Then $\mathcal{F}$ is a partition of Y into nonempty sets. Using the axiom of choice let $h : \mathcal{F} \to Y$ be a choice function. Define $g : Y \to X$ by $g(y) = h(f^{-1}[\{y\}])$. Then $g : Y \to X$ is injective.

(e) Use part (c) and the Schröder-Bernstein theorem. $\square$

(19) Prove the following.

(a) $|\mathbb{R}^\omega| = \mathfrak{c}$.

(b) $|C(\mathbb{R})| = \mathfrak{c}$ where $C(\mathbb{R})$ is the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

(c) Let A be the set of all real numbers which are roots of some polynomial equation with rational coefficients. Show that $|A| = \omega$.

Solution: (a) Let us write $X \sim Y$ iff there is a bijection from X to Y. Then it is easy to check that for any set A,

$$(A^\omega)^\omega \sim A^{\omega\times\omega} \sim A^\omega$$

Taking $A = 2 = \{0, 1\}$ and using the fact that $|\mathbb{R}| = |2^\omega| = \mathfrak{c}$, we get $|\mathbb{R}^\omega| = |(2^\omega)^\omega| = |2^\omega| = \mathfrak{c}$.

(b) It is clear that $|C(\mathbb{R})| \geq |\mathbb{R}| = \mathfrak{c}$ since every constant function is continuous. To show that $|C(\mathbb{R})| \leq \mathfrak{c}$, we'll construct an injective function from $C(\mathbb{R})$ to $\mathbb{R}^\omega$. This suffices since by part (a), $|\mathbb{R}^\omega| = \mathfrak{c}$. Since $|\mathbb{Q}| = \omega$, it is enough to construct an injective function $H : C(\mathbb{R}) \to \mathbb{R}^{\mathbb{Q}}$ where $\mathbb{R}^{\mathbb{Q}}$ is the set of all functions from $\mathbb{Q}$ to $\mathbb{R}$. Given $f \in C(\mathbb{R})$, define $H(f) = f \restriction \mathbb{Q}$. We claim that H is injective. To see this assume that $H(f) = H(g)$ and we'll show that $f = g$. Let $x \in \mathbb{R}$. Let $\langle a_n : n < \omega\rangle$ be a sequence of rationals converging to x. Since f, g are continuous, $f(a_n)$ converges to $f(x)$ and $g(a_n)$ converges to $g(x)$. As $f \restriction \mathbb{Q} = g \restriction \mathbb{Q}$, for every $n < \omega$ we must have $f(a_n) = g(a_n)$. Hence $f(x) = g(x)$. So $f = g$ and H is injective.

(c) For each $1 \leq n \leq \omega$, let P_n be the set of all polynomials of degree n with rational coefficients. The each polynomial $f \in P_n$ is of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_n, a_{n-1}, \ldots, a_0$ are in $\mathbb{Q}$ and $a_n \neq 0$. It follows that $|P_n| \leq |\mathbb{Q}^n| = \omega$. Let $A_n = \{a \in \mathbb{R} : (\exists p \in P_n)(p(a) = 0)\}$. Since each polynomial in P_n has $\leq n$ real roots, it follows that A_n is a countable union of finite sets. So each A_n is countable. Finally, $A = \bigcup\{A_n : 1 \leq n < \omega\}$ is a countable union of countable sets. Hence A is also countable. As every rational is in A, $|A| \geq \omega$. Hence $|A| = \omega$. $\square$

(20) Show that $\mathbb{R}^2$ cannot be partitioned into circles of positive radii.

Solution: Towards a contradiction suppose there is a partition $\mathcal{F}$ of $\mathbb{R}^2$ into circles of positive radii. Recursively construct $\langle (C_n, x_n) : n < \omega\rangle$ as follows.

(1) $C_0 \in \mathcal{F}$ is arbitrary and x_0 is the center of C_0.

(2) For each $n < \omega$, $C_{n+1} \in \mathcal{F}$ and $x_n \in C_{n+1}$.

Since $\mathcal{F}$ has pairwise disjoint circles, it is easy to see that each C_{n+1} lies completely inside C_n. Let r_n be the radius of C_n. Then $r_{n+1} < r_n/2$. It also follows that if $N < n \leq m < \omega$, then $||x_n - x_m|| \leq 2r_N$ (where $||x - y||$ is the distance between x and y). As $N \to \infty$, $r_N \to 0$. Hence $\langle x_n : n < \omega \rangle$ is a Cauchy sequence in $\mathbb{R}^2$. Let x be the limit of this sequence. Then $x \notin C_n$ because x lies inside every C_n. Since $\bigcup \mathcal{F} = \mathbb{R}^2$, there exists $C_\star \in \mathcal{F}$ such that $x \in C_\star$. Let $r_\star > 0$ be the radius of $C_\star$. Choose n large enough so that $r_n < r_\star/100$. Then it is clear that $C_\star \cap C_n \neq \emptyset$. But this contradicts the fact that $\mathcal{F}$ consists of pairwise disjoint circles. $\square$

(21) Show that $\mathbb{R}^3$ can be partitioned into circles of positive radii.

Solution: Let $\mathcal{C}$ be the family of all circles in $\mathbb{R}^3$. Let $\langle x_\alpha : \alpha < \mathfrak{c} \rangle$ be an injective sequence whose range is $\mathbb{R}^3$. Using transfinite recursion, construct $\langle \mathcal{C}_\alpha : \alpha < \mathfrak{c} \rangle$ such that the following hold.

(1) Each $\mathcal{C}_\alpha \subseteq \mathcal{C}$ consists of pairwise disjoint circles of positive radii and $\mathcal{C}_0 = \emptyset$.

(2) If $\alpha < \beta < \mathfrak{c}$, then $\mathcal{C}_\alpha \subseteq \mathcal{C}_\beta$.

(3) If $\alpha < \mathfrak{c}$ is limit, then $\mathcal{C}_\alpha = \bigcup \{\mathcal{C}_\beta : \beta < \alpha\}$.

(4) For every $\alpha < \mathfrak{c}$, $|\mathcal{C}_\alpha| \leq \max(\{\omega, |\alpha|\})$.

(5) For every $\alpha < \mathfrak{c}$, $x_\alpha \in \bigcup \mathcal{C}_{\alpha+1}$

At limit stages $\alpha < \mathfrak{c}$, we simply define $\mathcal{C}_\alpha$ by Clause (3) above. Having constructed $\mathcal{C}_\alpha$, $\mathcal{C}_{\alpha+1}$ is defined as follows. If $x_\alpha \in \bigcup \mathcal{C}_\alpha$, then we define $\mathcal{C}_{\alpha+1} = \mathcal{C}_\alpha$. Now assume that x_α does not lie on any circle in $\mathcal{C}_\alpha$.

Claim: There is a circle C such that C passes through x_α and for every circle $T \in \mathcal{C}_\alpha$, $T \cap C = \emptyset$.

Proof of Claim: Let $\mathcal{P}_\alpha$ be the family of all planes P such that some circle in $\mathcal{C}_\alpha$ lies completely within P. Then $|\mathcal{P}_\alpha| \leq |\mathcal{C}_\alpha| \leq \max(\{|\alpha|, \omega\}) < \mathfrak{c}$. Choose a plane P such that $x_\alpha \in P$ and $P \notin \mathcal{P}_\alpha$. This can be done because there are continuum many planes passing through x_α. Let B be the set of all points in P which also lie on some circle in $\mathcal{C}_\alpha$. Since each circle in $\mathcal{C}_\alpha$ meets P at ≤ 2 points, we get $|B| < \mathfrak{c}$. Note that $x_\alpha \notin B$ as $x_\alpha \notin \bigcup \mathcal{C}_\alpha$. Fix a line ℓ inside P that passes through x_α and consider the family $\mathcal{E}$ of all circles inside P which are tangent to ℓ at the point x_α. It is clear that $|\mathcal{E}| = \mathfrak{c}$ and any two circles in $\mathcal{E}$ meet exactly at x_α. Since $|B| < \mathfrak{c}$, we can find $C \in \mathcal{E}$ such that $C \cap B = \emptyset$. Then C is as required. $\square$

Let C be as in the claim. Define $\mathcal{C}_{\alpha+1} = \mathcal{C}_\alpha \cup \{C\}$ and note that $x_\alpha \in \bigcup \mathcal{C}_{\alpha+1}$. This completes the construction. Let $\mathcal{F} = \bigcup \{\mathcal{C}_\alpha : \alpha < \mathfrak{c}\}$. By Clause (1), it is clear that $\mathcal{F}$ is a disjoint family of circles. Also, by Clause (5), $\bigcup \mathcal{F} = \mathbb{R}^3$. Hence $\mathcal{F}$ is a partition of $\mathbb{R}^3$ into circles of positive radii. $\square$

(22) Suppose $A \subseteq \mathbb{R}^2$ and every vertical section of A is finite. Show that some horizontal section of $\mathbb{R}^2 \setminus A$ is uncountable.

Solution: For each $x \in \mathbb{R}$, define $W_x = A_x \cap \omega$. Then W_x is a finite subset of ω. Since $|\mathbb{R}| = \mathfrak{c} > \omega$ and there are only countably many finite subsets of ω, we can find a finite $W \subseteq \omega$ such that $Y = \{x \in \mathbb{R} : W_x = W\}$ has cardinality $\mathfrak{c}$. Fix $n \in \omega \setminus W$. Note that for every $x \in Y$, $(x, n) \notin A$. Now

$$(\mathbb{R}^2 \setminus A)^n = \{x \in \mathbb{R} : (x, n) \notin A\} \supseteq Y$$

Hence the horizontal section of $\mathbb{R}^2 \setminus A$ at n contains every member of Y. In particular, it is uncountable. $\square$

(23) Let ϕ be a propositional formula in which $\neg$ doesn't occur. Show that ϕ is satisfiable.

Solution: Let $val : \mathcal{V}ar \to \{0, 1\}$ be defined by $val(p) = 1$ for every propositional variable p. By induction on the length of ϕ, we will show $\mathbf{val}(\phi) = 1$ for every propositional formula in which $\neg$ doesn't occur.

If ϕ is a propositional variable, then this is clear.

Next assume that ϕ is of the form $\phi_1 \Box \phi_2$ where $\Box$ is one of the following connectives: $\wedge$, $\vee$, $\implies$, $\iff$. Note that $\neg$ doesn't occur in either one of ϕ_1 and ϕ_2. So by inductive hypothesis, $\mathbf{val}(\phi_1) = \mathbf{val}(\phi_2) = 1$. Now by the definition of $\mathbf{val}$, it easily follows that $\mathbf{val}(\phi) = 1$ in each of these cases. $\square$

(24) Suppose the set of propositional variables $\mathcal{V}ar$ is uncountable. Use Zorn's lemma to show the following: Let S be a set of propositional formulas such that every finite subset of S is satisfiable. Then S is satisfiable.

Solution: Let $\mathcal{F}$ be the set of all functions h such that $\text{dom}(h) \subseteq \mathcal{V}ar$, $\text{range}(h) \subseteq \{0, 1\}$ and for every finite $F \subseteq S$, there exists a valuation $val : \mathcal{V}ar \to \{0, 1\}$ such that $h \subseteq val$ and every formula in F is true under val.

We claim that every chain in $(\mathcal{F}, \subseteq)$ has an upper bound. To see this, fix an arbitrary chain $\mathcal{C} \subseteq \mathcal{F}$ and define $g = \bigcup \mathcal{C}$. Since $\mathcal{C}$ is a chain, it is easy to see that g is a function. Clearly, $\text{dom}(g) \subseteq \mathcal{V}ar$ and $\text{range}(g) \subseteq \{0, 1\}$. So it would be sufficient to show that $g \in \mathcal{F}$ since then g is an upper bound of $\mathcal{C}$ in $(\mathcal{F}, \subseteq)$. Towards a contradiction, suppose $g \notin \mathcal{F}$. Fix a finite $F \subseteq S$ such that there is no valuation $val : \mathcal{V}ar \to \{0, 1\}$ satisfying: $g \subseteq val$ and every formula in F is true under val. Choose a finite $V \subseteq \mathcal{V}ar$ that contains every propositional variable that occurs in a formula in F. Put $W = V \cap \text{dom}(g)$. Since $\mathcal{C}$ is a chain, we can find an $h \in \mathcal{C}$ such that $W \subseteq \text{dom}(h)$. Since $h \in \mathcal{F}$, there exists a valuation $val' : \mathcal{V}ar \to \{0, 1\}$ such that $h \subseteq val'$ and every formula in F is true under val'. Define another valuation $val : \mathcal{V}ar \to \{0, 1\}$ as follows:

$$val(p) = \begin{cases} g(p) & \text{if } p \in \text{dom}(g) \\ val'(p) & \text{otherwise} \end{cases}$$

Observe that val and val' agree on every propositional variable in V. Hence every formula in F is true under val. But $g \subseteq val$ so we have a contradiction. So $g \in \mathcal{F}$ is an upper bound of $\mathcal{C}$.

Using Zorn's lemma, fix a $\subseteq$-maximal f in $\mathcal{F}$. We claim that $\mathrm{dom}(f) = \mathcal{V}ar$. This will complete the proof since it implies that f is a valuation under which every formula in $\mathcal{F}$ is true. Towards a contradiction, assume some propositional variable $p \notin \mathrm{dom}(f)$. Define $f_0 = f \cup \{(p, 0)\}$ and $f_1 = \{(p, 1)\}$. By the Lemma on Lecture slide no. 98, it follows that one of f_0, f_1 is in $\mathcal{F}$. But this contradicts the maximality of g. Hence $\mathrm{dom}(f) = \mathcal{V}ar$ and the proof is complete. $\square$

(25) Let $\mathcal{L}, \mathcal{L}'$ be two first order languages where $\mathcal{L}'$ is obtained from $\mathcal{L}$ by adding a new constant symbol c to $\mathcal{L}$. Suppose T is an $\mathcal{L}$-theory, ϕ is an $\mathcal{L}$-formula with only free variable x, ψ is an $\mathcal{L}$-sentence and t is an $\mathcal{L}$-term with no variables. Show that the following hold.

(**UG**) If $T \vdash_{\mathcal{L}'} \phi(c/x)$, then $T \vdash_{\mathcal{L}} (\forall x)(\phi)$.

(**EI**) If $T \cup \{\phi(c/x)\} \vdash_{\mathcal{L}'} \psi$, then $T \cup \{(\exists x)(\phi)\} \vdash_{\mathcal{L}} \psi$.

Solution: Proof of (**UG**): Assume $T \vdash_{\mathcal{L}'} \phi(c/x)$ and fix a proof $\phi_1, \ldots, \phi_n$ of $\phi(c/x)$ in T where each ϕ_k is an $\mathcal{L}'$-sentence. Fix a variable v such that v does not occur in any of the formulas $\phi_1, \ldots, \phi_n$. Let ψ_k be the formula obtained by replacing every occurrence of c in ϕ_k by v. By induction on $k \leq n$, we'll show that $T \vdash_{\mathcal{L}} (\forall v)(\psi_k)$.

Case 1: $k = 1$. In this case, ϕ_1 must be either a logical axiom or a member of T. If $\phi_1 \in T$, then since c is not a symbol in $\mathcal{L}$, c doesn't occur in ϕ_1. So $\psi_1 = \phi_1$. Since $\psi_1 \implies (\forall v)(\psi_1)$ is a logical axiom of type 2, by Modus Ponens, it follows that $T \vdash_{\mathcal{L}} (\forall v)(\psi_1)$. Next suppose ϕ_1 is a logical axiom of one of the types 1-14. It is easily checked that in each one of these types, $(\forall v)(\psi_1)$ is also a logical axiom of the same type.

Case 2: $k > 1$. If ϕ_k is a logical axiom or a member of T, then $T \vdash_{\mathcal{L}} (\forall v)(\psi_k)$ follows from an argument similar to Case 1. Next suppose for some $i, j < k$, ϕ_j is $(\phi_i \implies \phi_k)$. Then $T \vdash_{\mathcal{L}} (\forall v)(\psi_k)$ by the following.

$T \vdash_{\mathcal{L}} (\forall v)(\psi_i)$ [Inductive hypothesis]

$T \vdash_{\mathcal{L}} (\forall v)(\psi_i \implies \psi_k)$ [Inductive hypothesis]

$T \vdash_{\mathcal{L}} (\forall v)(\psi_i \implies \psi_k) \implies ((\forall v)(\psi_i) \implies (\forall v)(\psi_k))$ [Type 3 axiom]

$T \vdash_{\mathcal{L}} (\forall v)(\psi_k)$ [Modus Ponens applied twice]

This completes the proof of $T \vdash_{\mathcal{L}} (\forall v)(\psi_k)$ for every $k \leq n$. Next, note that $(\forall v)(\phi(v/x)) \vdash_{\mathcal{L}} (\forall x)(\phi)$ by the following proof:

$(\forall v)(\phi(v/x))$ [Assumption]

$(\forall x)((\forall v)(\phi(v/x)) \implies \phi)$ [Type 4 axiom]

$(\forall x)[(\forall v)(\phi(v/x)) \implies \phi] \implies [(\forall x)(\forall v)(\phi(v/x)) \implies (\forall x)(\phi)]$ [Type 3 axiom]

$(\forall x)(\forall v)(\phi(v/x)) \implies (\forall x)(\phi)$ [Modus Ponens]

$(\forall v)(\phi(v/x)) \implies (\forall x)(\forall v)(\phi(v/x))$ [Type 2 axiom]

$(\forall x)(\forall v)(\phi(v/x))$ [Modus Ponens]

$(\forall x)(\phi)$ [Modus Ponens]

Since ψ_n is $\phi(v/x)$, by Modus Ponens, we get $T \vdash_{\mathcal{L}} (\forall x)(\phi)$. This completes the proof of (**UG**).

Proof of (**EI**): Assume $T \cup \{\phi(c/x)\} \vdash_{\mathcal{L}'} \psi$. Then $T \cup \{\neg\psi, \phi(c/x)\}$ is inconsistent. Hence $T \cup \{\neg\psi\} \vdash_{\mathcal{L}'} \neg\phi(c/x)$. Since ψ is an $\mathcal{L}$-sentence, $T \cup \{\neg\psi\}$ is an $\mathcal{L}$-theory. Applying (**UG**), we get $T \cup \{\neg\psi\} \vdash_{\mathcal{L}} (\forall x)(\neg\phi)$. Since $(\forall x)(\neg\phi) \iff \neg(\exists x)(\phi)$ is a logical axiom of type 6, it follows that $T \cup \{\neg\psi\} \vdash_{\mathcal{L}} \neg(\exists x)(\phi)$. So $T \cup \{(\exists x)(\phi), \neg\psi\}$ is inconsistent. Hence $T \cup \{(\exists x)(\phi)\} \vdash_{\mathcal{L}} \psi$. $\square$

(26) Suppose $\mathcal{L}, \mathcal{L}'$ are first order languages and $\mathcal{L}'$ extends $\mathcal{L}$. Let T be an $\mathcal{L}$-theory and ϕ be an $\mathcal{L}$-sentence. Then $T \vdash_{\mathcal{L}} \phi$ iff $T \vdash_{\mathcal{L}'} \phi$.

Solution sketch: That $T \vdash_{\mathcal{L}} \phi$ implies $T \vdash_{\mathcal{L}'} \phi$ is trivial. Next suppose $T \vdash_{\mathcal{L}'} \phi$ and fix a proof $\phi_1, \dots, \phi_n$ of ϕ in T where each ϕ_k is an $\mathcal{L}'$-sentence. **First assume that $\mathcal{L}$ has a constant symbol** and fix one such symbol c. For each $k \leq n$, define ψ_k as follows.

(a) Replace each atomic subformula of the form $R(t_1, \dots, t_m)$ of ϕ_k by $(\forall x)(x = x)$ where R is a relation symbol in $\mathcal{L}' \setminus \mathcal{L}$.

(b) Next, replace each constant symbol d in $\mathcal{L}' \setminus \mathcal{L}$ that occurs in ϕ_k by c.

(b) Finally, replace each term of the form $F(t_1, \dots, t_m)$ that occurs in ϕ_k by c where F is a function symbol in $\mathcal{L}' \setminus \mathcal{L}$.

It is clear that ψ_k is an $\mathcal{L}$-sentence. Now by induction on $k \leq n$, we can show that $T \vdash_{\mathcal{L}_1} \psi_k$. We omit the easy but tedious details. Note that since ϕ_n is ϕ and ϕ is an $\mathcal{L}$-sentence, ψ_n is same as ϕ and so $T \vdash_{\mathcal{L}} \phi$.

If $\mathcal{L}$ has no constant symbols, then we can define a new language $\mathcal{L}_1$ by adding a constant symbol c to $\mathcal{L}$. By the previous argument $T \vdash_{\mathcal{L}'} \phi$ implies $T \vdash_{\mathcal{L}_1} \phi$. Now $T \vdash_{\mathcal{L}} \phi$ easily follows from $T \vdash_{\mathcal{L}_1} \phi$ using (**UG**). $\square$

(27) Suppose T is a maximally consistent $\mathcal{L}$-theory and ϕ, ψ are $\mathcal{L}$-sentences. Show the following.

(a) $T \vdash \phi$ iff $\phi \in T$.

(b) $\neg\phi \in T$ iff $\phi \notin T$.

(c) $(\phi \wedge \psi) \in T$ iff $\phi \in T$ and $\psi \in T$.

(d) $(\phi \vee \psi) \in T$ iff either $\phi \in T$ or $\psi \in T$.

(e) $(\phi \implies \psi) \in T$ iff either $\psi \in T$ or $\phi \notin T$.

(f) $(\phi \iff \psi) \in T$ iff "$\phi \in T$ iff $\psi \in T$".

Solution:

(a) If $\phi \in T$, then $T \vdash \phi$. Next suppose $T \vdash \phi$. Then $T \cup \{\phi\}$ is consistent as T is consistent. Since T is maximally consistent, $T \cup \{\phi\} = T$. Hence $\phi \in T$.

(b) If $\neg\phi \in T$, then $\phi \notin T$ since T is consistent. Next suppose $\phi \notin T$. Then $T \cup \{\neg\phi\}$ is consistent. As T is maximally consistent, $T \cup \{\neg\phi\} = T$. Hence $\neg\phi \in T$.

(c) First suppose $\phi \in T$ and $\psi \in T$. Then $T \vdash \phi$ and $T \vdash \psi$. Since $(\phi \implies (\psi \implies (\phi \wedge \psi)))$ is a propositional tautology, by Modus Ponens, we get $T \vdash (\phi \wedge \psi)$. By part (a), $(\phi \wedge \psi) \in T$.

Next suppose $(\phi \wedge \psi) \in T$. Then $T \vdash (\phi \wedge \psi)$. Since $(\phi \wedge \psi) \implies \phi$ is a propositional tautology, by Modus Ponens, $T \vdash \phi$. Similarly, $T \vdash \psi$. By part (a), $\{\phi, \psi\} \subseteq T$.

(d) Suppose either $\phi \in T$ or $\psi \in T$. Since $(\phi \implies (\phi \vee \psi))$ and $(\psi \implies (\phi \vee \psi))$ are both propositional tautologies, by Modus Ponens, we get $(\phi \vee \psi) \in T$.

Next suppose $(\phi \vee \psi) \in T$ and $\phi \notin T$. Then by part (b), $\neg\phi \in T$. As $(\neg\phi \implies ((\phi \vee \psi) \implies \psi))$ is a propositional tautology, by Modus Ponens, $T \vdash \psi$. By part (a), $\psi \in T$.

(e) Since $((\phi \implies \psi) \implies (\neg\phi \vee \psi))$ and $((\neg\phi \vee \psi) \implies (\phi \implies \psi))$ are propositional tautologies, by Modus Ponens, we get $T \vdash (\phi \implies \psi)$ iff $T \vdash (\neg\phi \vee \psi)$. By part (a), this means that $(\phi \implies \psi) \in T$ iff $(\neg\phi \vee \psi) \in T$. By parts (b) and (d), it follows that $(\phi \implies \psi) \in T$ iff either $\psi \in T$ or $\phi \notin T$.

(f) First assume $(\phi \iff \psi) \in T$. Since $((\phi \iff \psi) \implies (\phi \implies \psi))$ and $(\phi \iff \psi) \implies (\psi \implies \phi))$ are propositional tautologies, by Modus Ponens, we get $T \vdash (\phi \implies \psi)$ and $T \vdash (\psi \implies \phi)$. Applying Modus Ponens again, this means $T \vdash \phi$ iff $T \vdash \psi$. By part (a), it follows that $\phi \in T$ iff $\psi \in T$.

Next suppose $\phi \in T$ iff $\psi \in T$. We will show $(\phi \iff \psi) \in T$. We consider the following two cases.

Case 1: Both ϕ and ψ are in T. By part (c), $T \vdash (\phi \wedge \psi)$. Since $((\phi \wedge \psi) \implies (\phi \iff \psi))$ is a propositional tautology, by Modus Ponens, we get $T \vdash (\phi \iff \psi)$. So by part (a), $(\phi \iff \psi) \in T$.

Case 2: Neither ϕ nor ψ is in T. By part (b), $\neg\phi \in T$ and $\neg\psi \in T$. By part (c), $T \vdash (\neg\phi \wedge \neg\psi)$. Since $((\neg\phi \wedge \neg\psi) \implies (\phi \iff \psi))$ is a propositional tautology, by Modus Ponens, we get $T \vdash (\phi \iff \psi)$. So by part (a), $(\phi \iff \psi) \in T$. $\square$

(28) Suppose T is a consistent complete $\mathcal{L}$-theory. Let S be the set all $\mathcal{L}$-sentences ϕ such that $T \vdash \phi$. Show that S is a maximally consistent $\mathcal{L}$-theory.

Solution: We first claim that for every $\mathcal{L}$-sentence ϕ, $T \vdash \phi$ iff $S \vdash \phi$. If $T \vdash \phi$, then $\phi \in S$ so clearly $S \vdash \phi$. Conversely, suppose $S \vdash \phi$ and fix a proof $\phi_1, \phi_2, \dots, \phi_n$ of ϕ in S. So ϕ_n is ϕ and each ϕ_i is either a logical axiom or a member of S or it was obtained from two sentences using Modus Ponens. If ϕ_i is a member of S, then $T \vdash \phi_i$. Let $\phi_{i,1}, \phi_{i,2}, \dots, \phi_{i,k(i)}$ be a proof of ϕ_i in T. In the sequence $\phi_1, \phi_2, \dots, \phi_n$, replace each $\phi_i \in S$ with the sequence $\phi_{i,1}, \phi_{i,2}, \dots, \phi_{i,k(i)}$. It is easy to see that this gives us a new sequence which is a proof of ϕ in T.

Since T is consistent, by the above claim, it follows that S is also consistent. Towards a contradiction, suppose S is not maximally consistent and fix an $\mathcal{L}$-sentence ϕ such that $\phi \notin S$ and $S \cup \{\phi\}$ is consistent. Since T is complete, either $T \vdash \phi$ or $T \vdash \neg\phi$. Since $\phi \notin S$, we cannot have $T \vdash \phi$. So $T \vdash \neg\phi$. Hence $\neg\phi \in S$. But this contradicts the fact that $S \cup \{\phi\}$ is consistent. Therefore S is a maximally consistent $\mathcal{L}$-theory. $\square$

(29) Let $\mathcal{L} = \mathcal{L}_{PA} \cup \{c\}$ where c is a new constant symbol. Let $\mathsf{Primes} = \{2, 3, 5, 7, \dots\}$ be the set of all primes numbers. For each $p \in \mathsf{Primes}$, let "p $\mathsf{divides}$ c" denote the $\mathcal{L}$-sentence $(\exists y)(S^p(0) \cdot y = c)$. For each $X \subseteq \mathsf{Primes}$, let T_X be the $\mathcal{L}$-theory

$$T_X = TA \cup \{(p \text{ divides } c) : p \in X\} \cup \{\neg(p \text{ divides } c) : p \in \mathsf{Primes} \setminus X\}$$

where $TA = Th(\omega, 0, S, +, \cdot)$ denotes true arithmetic.

(a) Show that T_X is consistent for every $X \subseteq \mathsf{Primes}$.

(b) Show that TA has continuum many pairwise non-isomorphic countable models.

Solution: (a) We will show that every finite subset of T_X has a model. This suffices since then, by compactness theorem, it will follows that T_X has a model and therefore T_X is consistent.

Let F be a finite subset of T_X. We will construct a model of F. Let W be the set of all primes p such that $(p \text{ divides } c) \in F$. Note that W is a finite subset of X. Let $\mathcal{M} = (\omega, 0, S, +, \cdot, c^{\mathcal{M}})$ where $(\omega, 0, S, +, \cdot)$ is the standard model of arithmetic and $c^{\mathcal{M}}$ is the product of all the primes in W (If $W = \emptyset$, then define $c^{\mathcal{M}} = 1$). Then a prime p divides $c^{\mathcal{M}}$ iff $p \in W$. It follows that $\mathcal{M} \models F$.

(b) Using part (a), we can fix a family $\{\mathcal{M}'_X : X \subseteq \mathsf{Primes}\}$ such that for each $X \subseteq \mathsf{Primes}$, $\mathcal{M}'_X = (M_X, 0^{\mathcal{M}_X}, S^{\mathcal{M}_X}, +^{\mathcal{M}_X}, \cdot^{\mathcal{M}_X}, c^{\mathcal{M}_X})$ is a countable $\mathcal{L}$-structure such that $\mathcal{M}'_X \models T_X$. Let $\mathcal{M}_X = (M_X, 0^{\mathcal{M}_X}, S^{\mathcal{M}_X}, +^{\mathcal{M}_X}, \cdot^{\mathcal{M}_X})$. Then $\mathcal{M}_X$ is an $\mathcal{L}_{PA}$-structure such that $\mathcal{M}_X \models TA$.

We claim that for any $X \subseteq \mathsf{Primes}$, $\{Y \subseteq \mathsf{Primes} : \mathcal{M}_X \cong \mathcal{M}_Y\}$ is countable. Since $|\{X : X \subseteq \mathsf{Primes}\}| = \mathfrak{c}$, it will follow that there are continuum many pairwise non-isomorphic models of TA in $\{\mathcal{M}_X : X \subseteq \mathsf{Primes}\}$.

Let $X \subseteq \mathsf{Primes}$. For each prime p, let ϕ_p denote the formula "p $\mathsf{divides}$ x" where x is a variable. For each $a \in M_X$, let $T_a = \{p \in \mathsf{Primes} : \mathcal{M}_X \models \phi_p(a/x)\}$. Then $\mathcal{T}_X = \{T_a : a \in M_X\}$ is a countable family of subsets of Primes.

Now observe that if $Y \subseteq \mathsf{Primes}$ and $Y \notin \mathcal{T}_X$, then $\mathcal{M}_X$ cannot be isomorphic to $\mathcal{M}_Y$. This is because there exists a member $a \in M_Y$ (namely, $a = c^{\mathcal{M}_Y}$) such that $Y = \{p \in \mathsf{Primes} : \mathcal{M}_Y \models \phi_p(a/x)\}$ while there is no such member in M_X. So $\{Y \subseteq \mathsf{Primes} : \mathcal{M}_X \cong \mathcal{M}_Y\}$ is countable and we are done. $\square$

(30) Show that every countable linear ordering is isomorphic to a subordering of the rationals $(\mathbb{Q}, <)$.

Solution: Let $(L, \prec)$ be a countable linear ordering. If L is finite, the result is clear so let us assume $|L| = \omega$. Let $L = \{a_0, a_1, a_2, \dots\}$ be a one-one enumeration of L. Inductively construct $\langle f_n : n < \omega \rangle$ such that the following hold.

(a) Each f_n is a finite function, $\mathrm{dom}(f_n) \subseteq L$ and $\mathrm{range}(f_n) \subseteq \mathbb{Q}$.

(b) For every a, a' in $\mathrm{dom}(f_n)$, $a \prec a'$ iff $f(a) < f(a')$.

(c) For every $n < \omega$, $a_n \in \mathrm{dom}(f_n)$.

Start by defining $f_0 = \{(a_0, 0)\}$.

Having defined f_n, define f_{n+1} as follows: If $a_{n+1} \in \mathrm{dom}(f_n)$, then $f_{n+1} = f_n$. So assume $a_{n+1} \notin \mathrm{dom}(f_n)$. Put $Left = \{a \in \mathrm{dom}(f_n) : a \prec a_{n+1}\}$ and $Right = \{a \in \mathrm{dom}(f_n) : a_{n+1} \prec a\}$. Let $L = \{f(a) : a \in Left\}$ and $R = \{f(a) : a \in Right\}$. Then L, R are finite subsets of $\mathbb{Q}$ and every member of L is less than every member of R. Since $(\mathbb{Q}, <)$ is a dense linear ordering without end-points, we can choose $b \in \mathbb{Q} \setminus \mathrm{range}(f_n)$ such that for every $x \in L$ and $y \in R$, $x < b$ and $b < y$. Define $f_{n+1} = f_n \cup \{(a_{n+1}, b)\}$. It is clear that clauses (a), (b) and (c) are preserved.

Finally, put $f = \bigcup\{f_n : n < \omega\}$. Then $f : L \to \mathbb{Q}$ is an order preserving function. Hence $(L, \prec)$ is isomorphic to $(\mathrm{range}(f), <)$. $\square$

(31) Let $W \subseteq \omega$ be nonempty. Show that W is c.e. iff there exists a computable function $f : \omega \to \omega$ such that $\mathrm{range}(f) = W$.

Solution: First assume that W is c.e. Fix a program P such that for each $n < \omega$, P halts on input n iff $n \in W$.

Define a program Q as follows. On input n, Q runs P on each one of the inputs $0, 1, \ldots, n$ for n steps. Let S_n be the set of those $k \leq n$ such that P halts on input k in at most n steps. Let W_n be the set of outputs of Q on inputs $0, 1, \ldots, n-1$. If $S_n \setminus W_n \neq \emptyset$, then Q outputs $\min(S_n \setminus W_n)$. Otherwise, Q outputs $\min(W)$.

It is clear that Q halts on every input. Let $f : \omega \to \omega$ be the function computed by Q. We claim that $\mathrm{range}(f) = W$. That $\mathrm{range}(f) \subseteq W$ is obvious. For the other inclusion, towards a contradiction, suppose $W \setminus \mathrm{range}(f) \neq \emptyset$ and let $n_\star = \min(W \setminus \mathrm{range}(f))$. Choose $m > n_\star$ large enough such that $W \cap n_\star \subseteq \mathrm{range}(f \restriction m)$ and for every $n \leq n_\star$, if $n \in W$, then P halts on input n is less than m steps. Now observe that on input m, Q must output $n_\star$: A contradiction. So we must have $W \subseteq \mathrm{range}(f)$. It follows that $W = \mathrm{range}(f)$.

Next assume that $f : \omega \to \omega$ is computable. Put $W = \mathrm{range}(f)$. Let P be a program that on input n starts computing $f(0), f(1), f(2), \ldots$ and halts iff n appears in this list. Then P witnesses that W is c.e. $\square$

(32) Suppose $r_1, r_2, \ldots, r_n, d_1, d_2, \ldots, d_n$ are natural numbers and for every $1 \leq i \leq n$, $0 \leq r_i < d_i$. Assume that for every $1 \leq i < j \leq n$, d_i and d_j are relatively prime. Show that there exists a positive integer N such that for every $1 \leq i \leq n$, $rem(N, d_i) = r_i$.

Solution: Let $D = d_1 d_2 \dots d_n$ and for each $1 \le i \le n$, $D_i = D/d_i$. Then $\mathsf{GCD}(D_i, d_i) = 1$ so there are integers M_i, m_i such that $M_i D_i + m_i d_i = 1$. Define

$$x = \sum_{1 \le i \le n} r_i M_i D_i$$

Since

$$x - r_j = r_j(M_j D_j - 1) + \sum_{1 \le i \le n}^{i \ne j} r_i M_i D_i = -r_j m_j d_j + \sum_{1 \le i \le n}^{i \ne j} r_i M_i D_i$$

it follows that d_j divides $x - r_j$ for every $1 \le j \le n$. Let $N = x + D(1 + |x|)$. Then $N \ge 1$ is as required. □

(33) Let $W \subseteq \omega$ be nonempty. Show that W is c.e. iff there exists a computable $A \subseteq \omega^2$ such that $W = \{n \in \omega : (\exists m)((n, m) \in A)\}$.

Solution: First assume that W is c.e. By problem (31), we can fix a computable function $f : \omega \to \omega$ such that range$(f) = W$. Define $A = \{(f(m), m) : m < \omega\}$. Then $A \subseteq \omega^2$ is computable and $W = \{n : (\exists m)((n, m) \in A)\}$.

Next suppose $A \subseteq \omega^2$ is computable and $W = \{n : (\exists m)((n, m) \in A)\}$. Let P be a program that computes A. Consider a program Q that on input n starts running P with inputs $(n, 0), (n, 1), (n, 2), \dots$ and halts as soon as P returns 1 on any of these inputs. It is clear that Q halts on input n iff $n \in W$. So W is c.e. □

(34) Suppose $X \subseteq \omega$ is numeralwise representable in PA. Show that X is computable.

Solution: Fix an $\mathcal{L}_{PA}$ formula $\phi(x)$ such that for every $n < \omega$, if $n \in A$, then $PA \vdash \phi(\overline{n})$ and if $n \notin A$, then $PA \vdash \neg\phi(\overline{n})$. Since the set of theorems in PA is c.e. (see Slides 186-187), we can fix a program P such that for any $\mathcal{L}_{PA}$-sentence ψ, P halts on input ψ iff $PA \vdash \psi$. Consider the program Q which on input n, runs P with inputs $\phi(\overline{n})$ and $\neg\phi(\overline{n})$. If P halts on input $\phi(\overline{n})$, then Q returns 1. If P halts on input $\neg\phi(\overline{n})$, then Q returns 0. It is easy to see that Q computes X. □

(35) Let $H \subseteq \omega$ be a non-computable c.e. set. Show that H is definable in $\mathcal{N} = (\omega, 0, S, +, \cdot)$ but not numeralwise representable in PA.

Solution: By problem (33), we can fix a computable $A \subseteq \omega^2$ such that $H = \{n : (\exists m)((n, m) \in A)\}$. Since H is computable, it is definable in $\mathcal{N}$. So there is an $\mathcal{L}_{PA}$-formula $\phi(y, x)$ such that for every $(n, m) \in \omega^2$, $(n, m) \in A$ iff $\mathcal{N} \models \phi(n, m)$. Let $\psi(y)$ be the formula $(\exists x)(\phi(y, x))$. Then for every $n < \omega$, $n \in H$ iff $(\exists m)((n, m) \in A)$ iff $\mathcal{N} \models \psi(n)$. Hence H is definable in $\mathcal{N}$ via $\psi(y)$. That H is not numeralwise representable in PA follows from problem (34) and the fact that H is non-computable. □

(36) Do the Exercise on Lecture slide 202.

Solution: Let $m < \omega$. We must show that if $m \in H$, then Q returns 1 on input m and if $m \notin H$, then Q returns 0 on input m.

First suppose $m \in H$. Then for some $n < \omega$, $f(n) = m$. By Clause 1, $PA \vdash \psi(\overline{m}, \overline{n})$. Note that $\psi(\overline{m}, \overline{n}) \implies (\exists x)(\psi(\overline{m}, x))$ is a logical axiom of type 5. So by Modus Ponens, $PA \vdash (\exists x)(\psi(\overline{m}, x))$. Hence Q returns 1 on input m.

Next suppose $m \notin H$. We must show that $PA \nvdash (\exists x)(\psi(\overline{m}, x))$. Towards a contradiction, suppose $PA \vdash (\exists x)(\psi(\overline{m}, x))$. Since $\mathcal{N}$ is a model of PA, it follows that $\mathcal{N} \models (\exists x)(\psi(m, x))$. Fix $n < \omega$ such that $\mathcal{N} \models \psi(m, n)$. Since $m \notin H = \text{range}(f)$, we must have $f(n) \neq m$. By Clause 2, this implies that $PA \vdash \neg\psi(\overline{m}, \overline{n})$. As $\mathcal{N}$ models PA, we get $\mathcal{N} \models \psi(m, n)$. So $\mathcal{N} \models \psi(m, n)$ and $\mathcal{N} \models \neg\psi(m, n)$: A contradiction.

It follows that Q computes H. $\square$