MAU22C00: PRACTICE EXAM 2020

1)

(a) Let A and B be sets, and let $f : A \to B$ be a function. Assume the set A is finite. Prove that the function f is injective $\iff$ the set $f(A)$ has the same number of elements as A.

(b) For $x, y \in \mathbb{R}$, xRy if and only if $x^2 = y^2$. Determine the following:

(i) Whether or not the relation R is *reflexive*;
(ii) Whether or not the relation R is *symmetric*;
(iii) Whether or not the relation R is *anti-symmetric*;
(iv) Whether or not the relation R is *transitive*;
(v) Whether or not the relation R is an *equivalence relation*;
(vi) Whether or not the relation R is a *partial order*.
(vii) If R is an equivalence relation, what the equivalence class of each $x \in \mathbb{R}$ is.

Give appropriate short proofs and/or counterexamples to justify your answer.

Solution: 1(a) The statement to be proven is an equivalence, so it can be proved in one of two ways, either proving each implication separately or traveling along a chain of statements that are equivalent. The latter is the easiest way for this problem. A is finite so we can write it as $A = \{a_1, a_2, ..., a_p\}$ for some p. Then $f(A) = \{f(a_1), f(a_2), ..., f(a_p)\} \subseteq B$. A priori, some $f(a_i)$ might be the same as some $f(a_j)$. However, f injective $\Leftrightarrow$ $f(a_i) \neq f(a_j)$ whenever $i \neq j$ $\Leftrightarrow$ $f(A)$ has exactly p elements just like A.

1(b) part (i) For every $x \in \mathbb{R}$, $x^2 = x^2$ so xRx, therefore the relation R is reflexive.

(ii) If xRy, then $x^2 = y^2$, hence $y^2 = x^2$ because equality is symmetric. Therefore, yRx as needed. Thus, the relation R is symmetric.

(iii) If xRy and yRx, then $x^2 = y^2$ (and $y^2 = x^2$, which amounts to the same thing). Since $x^2 = y^2 \iff x^2 - y^2 = (x-y)(x+y) = 0$, we obtain $x = y$ or $x = -y$. In other words, xRy and yRx are simultaneously satisfied if $x = -y$, which means R is not anti-symmetric. By the way, resist the temptation of stating that if a relation is symmetric it cannot be antisymmetric. That statement is false. Equality is a relation that is both symmetric and anti-symmetric.

(iv) If xRy and yRz, then $x^2 = y^2$ and $y^2 = z^2$, which means $x^2 = z^2$ because equality is transitive. Therefore, xRz as needed, so R is transitive.

(v) Since R is reflexive, symmetric, and transitive as established above, it is an equivalence relation.

(vi) Since R is reflexive and transitive, but it is not anti-symmetric as established above, R is not a partial order.

(vii) Recall that the equivalence class of an element $x \in \mathbb{R}$ is given by $[x]_R = \{y \in \mathbb{R} \mid xRy\}$. In this case, $xRy \iff x^2 = y^2$. Therefore, we want to find all real numbers, which squared equal x^2. It turns out we can use work carried out in a previous part, namely $x^2 = y^2 \iff x = y$ or $x = -y$. We conclude that $\forall\, x \in \mathbb{R}$, $[x]_R = \{x, -x\}$. The real numbers x and $-x$ are distinct whenever $x \neq 0$, so the equivalence relation R partitions the real numbers $\mathbb{R}$ into uncountably infinitely many two-element equivalence classes $\{x, -x\}$ and one equivalence class consisting of a single element $\{0\}$ as $0 = -0$. Note that the set of two-element equivalence classes is uncountably infinite because it contains as a subset $\{[x]_R \mid x \in (0, 1)\}$ and we proved in lecture that the set $(0, 1)$ is uncountably infinite.

2) Let $A = \left\{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}, 1\right\} \subset \mathbb{C}$ with the operation of multiplication.

(a) Is $(A, \cdot)$ a semigroup? Justify your answer.
(b) Is $(A, \cdot)$ a monoid? Justify your answer.
(c) Is $(A, \cdot)$ a group? Justify your answer.
(d) Write down four isomorphisms from A to itself.

Solution: 2(a) Yes, $(A, \cdot)$ is a semi-group. $1 = e^{\frac{10\pi i}{5}} = e^{2\pi i}$. In fact, $e^{2k\pi i} = 1$ for every $k \in \mathbb{Z}$. Therefore, $A = \left\{e^{\frac{2k\pi i}{5}} \mid k \in \mathbb{Z}\right\}$. $\forall\, a, b \in A$, $a = e^{\frac{2k\pi i}{5}}$ for some $k \in \mathbb{Z}$ and $b = e^{\frac{2l\pi i}{5}}$ for some $l \in \mathbb{Z}$. Therefore, $a \cdot b = e^{\frac{2k\pi i}{5}} \cdot e^{\frac{2l\pi i}{5}} = e^{\frac{2k\pi i + 2l\pi i}{5}} = e^{\frac{2(k+l)\pi i}{5}} \in A$ because as shown in lecture $k, l \in \mathbb{Z} \implies k + l \in \mathbb{Z}$. We conclude that multiplication on A is a binary operation. To prove that multiplication is associative on A, we choose any $a, b, c \in A$. Then $a = e^{\frac{2k\pi i}{5}}$, $b = e^{\frac{2l\pi i}{5}}$, $c = e^{\frac{2m\pi i}{5}}$ for some $k, l, m \in \mathbb{Z}$.

$$a\cdot(b\cdot c) = e^{\frac{2k\pi i}{5}}\cdot(e^{\frac{2l\pi i}{5}}\cdot e^{\frac{2m\pi i}{5}}) = e^{\frac{2k\pi i}{5}}\cdot e^{\frac{2l\pi i}{5}}\cdot e^{\frac{2m\pi i}{5}} = e^{\frac{2(k+l+m)\pi i}{5}} = (e^{\frac{2k\pi i}{5}}\cdot e^{\frac{2l\pi i}{5}})\cdot e^{\frac{2m\pi i}{5}}.$$

A set endowed with an associative binary operation is by definition a semi-group.

(b) $1 \in A$, and 1 is the multiplicative identity for $\mathbb{C}$, where $A \subset \mathbb{C}$. We conclude that 1 is the multiplicative identity of A. One can also check directly that for every $e^{\frac{2k\pi i}{5}} \in A$, $e^{\frac{2k\pi i}{5}} \cdot 1 = 1 \cdot e^{\frac{2k\pi i}{5}} = e^{\frac{2k\pi i}{5}}$. $(A, \cdot)$ is thus a semi-group with an identity element, hence a monoid by definition.

(c) Since we have shown that $(A, \cdot)$ is a monoid, we only need to show each element of A is invertible. Indeed, $1 = 1 \cdot 1 = 1$, 1 is its own inverse. $e^{\frac{2\pi i}{5}} \cdot e^{\frac{8\pi i}{5}} = e^{\frac{10\pi i}{5}} = 1 = e^{\frac{8\pi i}{5}} \cdot e^{\frac{2\pi i}{5}}$. We conclude that $e^{\frac{8\pi i}{5}}$ is the inverse of $e^{\frac{2\pi i}{5}}$ and $e^{\frac{2\pi i}{5}}$ is the inverse of $e^{\frac{8\pi i}{5}}$. Similarly, $e^{\frac{4\pi i}{5}} \cdot e^{\frac{6\pi i}{5}} = e^{\frac{6\pi i}{5}} \cdot e^{\frac{4\pi i}{5}} = e^{\frac{10\pi i}{5}} = 1$. Therefore, $e^{\frac{4\pi i}{5}}$ is the inverse of $e^{\frac{6\pi i}{5}}$ and $e^{\frac{6\pi i}{5}}$ is the inverse of $e^{\frac{4\pi i}{5}}$. We have shown that all elements of A are invertible, so $(A, \cdot)$ is a group.

(d) An isomorphism from A to itself is a bijective map $\varphi : A \to A$ that respects the binary operation. In other words, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for every $a, b \in A$. The easiest isomorphism from A to itself to write down is the identity map, which is given by $\varphi_1(a) = a$ for every $a \in A$. Before we write down three other isomorphisms, we need to understand a bit more about the structure of A. Let $a = e^{\frac{2\pi i}{5}}$. We immediately see that $A = \{a, a^2, a^3, a^4, 1\}$, where $1 = a^5$. In other words, $(A, \cdot)$ is a finite cyclic group with five elements. We could then define another isomorphism by $\varphi_2(a) = a^2$. It turns out that it suffices to specify where we send the generator a as this specifies the isomorphism completely. Indeed, $\varphi_2(a^2) = \varphi_2(a) \cdot \varphi_2(a) = a^2 \cdot a^2 = a^4$. $\varphi_2(a^3) = \varphi_2(a^2) \cdot \varphi_2(a) = a^4 \cdot a^2 = a^6 = a$ since $a^5 = 1$. $\varphi_2(a^4) = \varphi_2(a^3) \cdot \varphi_2(a) = a \cdot a^2 = a^3$. Finally, an isomorphism must send the identity element to itself, so $\varphi_2(1) = 1$. Similarly, we see that setting $\varphi_3(a) = a^3$ specifies another isomorphism. Finally, we set $\varphi_4(a) = a^4$. Check on your own that φ_3 and φ_4 are isomorphisms by checking where the other elements of A are sent, hence checking that the result is a bijection that respects the binary operation as we did for φ_2.

3) Let L be the language over the alphabet $A = \{a, l, p\}$ consisting of all words containing at least one of the substrings pl or la.

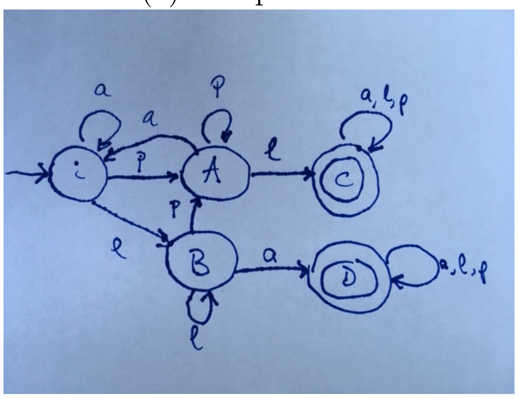
(a) Draw a finite state acceptor that accepts the language L. Carefully label all the states including the starting state and the finishing states as well as all the transitions.

(b) Devise a regular grammar in normal form that generates the language L. Be sure to specify the start symbol, the non-terminals, and all the production rules.

(c) Write down a regular expression that gives the language L and justify your answer.

(d) Let M be the set of languages L' over the alphabet $A = \{a, l, p\}$ satisfying that $L \cap L' \neq \emptyset$. Is M finite, countably infinite or uncountably infinite? Justify your answer.

Solution: 3(a) The picture is below.



(b) The regular grammar in normal form corresponding to the finite state acceptor drawn is the following:

(1) $\langle S\rangle \to a\langle S\rangle$.
(2) $\langle S\rangle \to p\langle A\rangle$.
(3) $\langle S\rangle \to l\langle B\rangle$.
(4) $\langle A\rangle \to a\langle S\rangle$.
(5) $\langle A\rangle \to p\langle A\rangle$.
(6) $\langle A\rangle \to l\langle C\rangle$.
(7) $\langle C\rangle \to a\langle C\rangle$.
(8) $\langle C\rangle \to l\langle C\rangle$.
(9) $\langle C\rangle \to p\langle C\rangle$.
(10) $\langle B\rangle \to l\langle B\rangle$.
(11) $\langle B\rangle \to p\langle A\rangle$.
(12) $\langle B\rangle \to a\langle D\rangle$.
(13) $\langle D\rangle \to a\langle D\rangle$.
(14) $\langle D\rangle \to l\langle D\rangle$.
(15) $\langle D\rangle \to p\langle D\rangle$.
(16) $\langle C\rangle \to \epsilon$.
(17) $\langle D\rangle \to \epsilon$.

(c) The regular expression $(A^* \circ p \circ l \circ A^*) \cup (A^* \circ l \circ a \circ A^*)$ generates L as the first parenthesis gives all strings with pl as a substring, while the second parenthesis gives all strings with la as a substring.

(d) The set M has as a subset $\tilde{M}$ consisting of all languages L' over the alphabet $A = \{a, l, p\}$ such that $L' = L' \cap L \neq \emptyset$. In other words, $\tilde{M}$ consists of all non-empty sublanguages of L. If we can prove that $\tilde{M}$ is uncountably infinite, then M would itself be uncountably infinite as it would have an uncountably infinite subset. To determine the size of $\tilde{M}$, we must first figure out what the size of L is. We proved in lecture that since the alphabet A is finite, the set of all words over A, namely A^*, is countably infinite. We know that $L \subset A^*$, so L must either be finite or countably infinite. In fact, all strings pla^m for $m \geq 0$ are in L. Thus the set B consisting of these strings $B = \{pla^m \bigm| m \in \mathbb{N}\} \subset L$. We can set up a bijection $f : \mathbb{N} \to B$ as follows $f(m) = pla^m$ (check it is a bijection!), so B is in one-to-one correspondence with $\mathbb{N}$, which we proved in lecture is countably infinite. Therefore, L can be either finite or countably infinite as we concluded before <u>and</u> L contains a subset B, which is countably infinite. Therefore, L is countably infinite. Therefore, $L \sim \mathbb{N}$, but then the set of subsets of of L, the power set of L, which we denoted by $\mathcal{P}(L)$, is in one-to-one correspondence to the power set of $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, which we proved in class is uncountably infinite. Therefore, $\mathcal{P}(L)$ is uncountably infinite. $\tilde{M}$ consists only of the non-empty sublanguages of L, so $\tilde{M} = \mathcal{P}(L)\backslash\{\emptyset\}$. If we take an uncountably infinite set and remove one of its elements, it stays uncountably infinite. Therefore, $\tilde{M}$ is uncountably infinite, but $\tilde{M} \subset M$. Therefore, M must be uncountably infinite.

4) In this question, all graphs are undirected graphs.

(a) Let (V, E) be the graph with vertices a, b, c, d, e, f, and g, and edges ab, ac, cd, bd, de, dg, ef and fg.
  - (i) Draw this graph. Write down its incidence table and its adjacency table.
  - (ii) Is this graph complete? Justify your answer.
  - (iii) Is this graph bipartite? Justify your answer.
  - (iv) Does this graph have an Eulerian circuit? Justify your answer.
  - (v) Does this graph have a Hamiltonian trail? Justify your answer.
  - (vi) Is this graph a tree? Justify your answer.

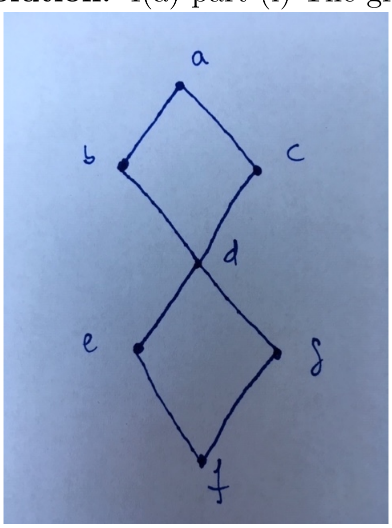
(b) Let (V, E) be the graph defined in part (a). Give an example of an isomorphism $\varphi : V \to V$ from the graph (V, E) to itself that satisfies $\varphi(b) = e$.

(c) Consider the connected undirected graph with vertices A, B, C, D, E, F, G, H, I, J, K, and L, and with edges listed with associated costs in the following table:

JK	EF	BH	DE	AD	IJ	BL	CE	HG	FH
1	2	2	3	3	4	5	5	6	7
AB	FJ	GK	EI	EJ	CD	CF	HL	AC	BC
7	8	8	9	10	11	12	12	13	14

Draw the graph labelling each edge with its cost, then determine the minimum spanning tree of this graph generated by Kruskal's Algorithm, where that algorithm is applied with the queue specified in the table above. For each step of the algorithm, write down the edge that is added.

Solution: 4(a) part (i) The graph is below.



The incidence table is

	ab	ac	cd	bd	de	dg	ef	fg
a	1	1	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0
c	0	1	1	0	0	0	0	0
d	0	0	1	1	1	1	0	0
e	0	0	0	0	1	0	1	0
f	0	0	0	0	0	0	1	1
g	0	0	0	0	0	1	0	1

The adjacency table is

	a	b	c	d	e	f	g
a	0	1	1	0	0	0	0
b	1	0	0	1	0	0	0
c	1	0	0	1	0	0	0
d	0	1	1	0	1	0	1
e	0	0	0	1	0	1	0
f	0	0	0	0	1	0	1
g	0	0	0	1	0	1	0

(ii) No, for example edge af is not part of the graph.

(iii) Yes, the set of vertices can be divided into two disjoint sets $\{a, d, f\}$ and $\{b, c, e, g\}$ such that each edge goes from a vertex in one set to a vertex in the other set.

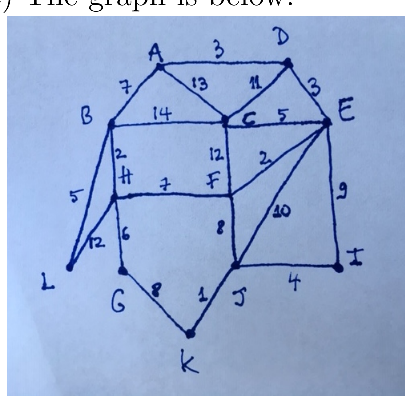
(iv) Yes, every vertex has even degree. In fact, for this graph, it is very easy to see what the Eulerian circuit needs to be: abdefgdca.

(v) Yes, but we need to avoid going through vertex d twice as the graph consists of two rhombuses attached at vertex d. For example, cabdefg is a Hamiltonian trail.

(vi) No, the graph consists of two rhombuses attached at vertex d, and each rhombus constitutes a circuit.

(b) To specify what an isomorphism does, we need to specify where it sends each of the vertices. Due to the edges in the graph, $\varphi(b) = e$ forces $\varphi(a) = f$, $\varphi(d) = d$, and $\varphi(c) = g$. As result, $\varphi(e) = b$, $\varphi(g) = c$, and $\varphi(f) = a$.

(c) The graph is below.



The edges are added in the following order in Kruskal's Algorithm: JK, EF, BH, DE, AD, IJ, BL, CE, HG, FH, and FJ.

5)

(a) Is the set of all integers divisible by 11 finite, countably infinite, or uncountably infinite? Justify your answer.
(b) Is $\{(x,y) \in \mathbb{R}^2 \big| y = e^x\}$ finite, countably infinite, or uncountably infinite? Justify your answer.
(c) Is $\{z \in \mathbb{C} \mid z^8 + 5z^6 - 3z^2 + 1 = 0\}$ finite, countably infinite, or uncountably infinite? Justify your answer.
(d) Let A be a finite alphabet. Prove that the set of all Turing-decidable languages over A is countably infinite.

Solution: 5(a) Let A be the set of all integers divisible by 11. The map $f : \mathbb{Z} \to A$ given by $f(m) = 11m$ for $m \in \mathbb{Z}$ is a bijection (check!). As proven in class, $\mathbb{Z}$ is countably infinite, so the set of all integers divisible by 11 is countably infinite.

(b) $A = \{(x,y) \in \mathbb{R}^2 \mid y = e^x\}$ is uncountably infinite. We proved in class that $(0,1)$ is uncountably infinite. The map $f : (0,1) \to \mathbb{R}$ defined by $f(x) = e^x$ gives us a bijection between $(0,1)$ and the subset of A given by $A \cap ((0,1) \times \mathbb{R})$. Therefore, $A \cap ((0,1) \times \mathbb{R})$ is uncountably infinite, which means A must be as well.

(c) $A = \{z \in \mathbb{C} \mid z^8 + 5z^6 - 3z^2 + 1 = 0\}$ is finite. By the Fundamental Theorem of Algebra, the complex polynomial of degree 8 given by $z^8 + 5z^6 - 3z^2 + 1 = 0$ has 8 roots in $\mathbb{C}$ counted with multiplicity, so at most 8 points in $\mathbb{C}$ satisfy $z^8 + 5z^6 - 3z^2 + 1 = 0$ and are hence in A.

(d) Let B be the set of all Turing-decidable languages over the alphabet A. We proved in lecture that the set of Turing-recognisable languages is countably infinite. Every Turing-decidable language is Turing-recognisable, so B is the subset of a countably infinite set. As a result, B can be finite or countably infinite. We will show that B is countably infinite. Indeed, every regular language is Turing-decidable because it is accepted by a finite state acceptor, which we can transform into a decider. As we proved in class, the set of all regular languages over a finite alphabet is countably infinite. We conclude that B has a countably infinite subset of its own, so B is contained in a countably infinite set and contains a countably infinite set. Therefore, B must be countably infinite.

6)

(a) Consider the language L over the alphabet $A = \{a, l, p\}$ consisting of all words of the form $ppa^m l^{3m}$ for $m \in \mathbb{N}^*$. Use the Pumping Lemma to show the language L is not regular.

(b) Consider the language over the binary alphabet $A = \{0, 1\}$ given by

$$L = \{0^m 1^{m+1} \mid m \in \mathbb{N},\ m \geq 0\}.$$

Write down the algorithm of a Turing machine that recognizes L. Process the following strings according to your algorithm: 1, 01, 011, and 010.

(c) Let A be a finite alphabet, and let P, Q, and R be three languages over the alphabet A. If P is Turing-recognisable, then Q is Turing-recognisable. If Q is Turing-recognisable, then P is Turing-recognisable and R is Turing-recognisable. R not Turing-recognisable is equivalent to P being Turing-recognisable. Prove that P is not Turing-recognisable.

Solution: 6(a) If L is a regular language, then it has a pumping length P. Consider $w = ppa^P l^{3P} \in L$. According to the Pumping Lemma, w is to be decomposed as xuy, where $|u| \geq 1$ and $|xu| \leq P$. Since $|xu| \leq P$, u can consists of only a's or one p and the rest a's. In other words, we have chosen w in such as way as to eliminate the possibility of u containing l's.

Case 1: u consists only of a's. Then, $x = ppa^{n_1}$, $u = a^{n_2}$, where $n_1 + n_2 \leq P - 2$; $n_1, n_2 \in \mathbb{N}$. Clearly, $xu^2y \notin L$ as $n_2 \geq 1$, so the number of a's in xu^2y is larger than one third the number of l's.

Case 2: u consists of one p and the rest a's. Then, $x = p$ and $u = pa^m$ with $0 \leq m \leq P - 2$. Clearly, $xu^2y \notin L$ as it contains two p's followed by a sequence of a's followed by a p followed by a sequence of a's and finally a sequence of l's. This violates the pattern of the language.

We conclude that the pumping length cannot exist, so L is not regular.

(b) Here is the algorithm for recognising $L = \{0^m 1^{m+1} \mid m \in \mathbb{N}, m \geq 0\}$.

(1) If the first cell is blank, then REJECT. If 1 is in the first cell, then move right. If the current cell is blank, then ACCEPT; otherwise, REJECT. Proceed to step 2.
(2) If 0 is in the current cell, delete it, then move right to the first 1.
(3) If there is no first 1, REJECT. Otherwise change 1 to x.
(4) Move to the leftmost non blank symbol. If 0, go to step 2. If 1, REJECT. If x, go to step 5.

(5) Move right until a character other than x is detected. If this character is 0 or blank, then REJECT; otherwise, go to the next step.
(6) If the character in the current cell is 1, then move right. If the current cell is blank, then ACCEPT; otherwise, REJECT.

Here is how the following strings are treated:

- 1 is accepted immediately at step 1.
- $01 \to \llcorner 1 \to \llcorner x \to$ REJECT at step 5.
- $011 \to \llcorner 11 \to \llcorner x1 \to$ ACCEPT at step 6.
- $010 \to \llcorner 10 \to \llcorner x0 \to$ REJECT at step 5.

(c) This part of the problem is in fact a propositional logic problem in the guise of a problem about Turing-recognisable languages. As a shorthand, we will denote by 'P' the statement 'P is Turing-recognisable,' by 'Q' the statement 'Q is Turing-recognisable,' and by 'R' the statement 'R is Turing-recognisable,' The given hypotheses are:
(a) $P \to Q$
(b) $Q \to (P \wedge R)$
(c) $\neg R \leftrightarrow P$

We wish to prove $\neg P$. We do so as follows:

(1) $Q \to (\neg R \wedge R)$ substitution of (c) into (b).
(2) $\neg(\neg R \wedge R) \to \neg Q$ contrapositive of (1) (tautology #24 on the list of tautologies posted in Course Documents)
(3) $R \vee \neg R$ law of the excluded middle (tautology #1 on the list of tautologies)
(4) $\neg(\neg R \wedge R)$ De Morgan's law applied to (3) (tautology #18) and substitution of $\neg(\neg R)$ by R by the law of double negation (tautology #3)
(5) $\neg Q$ modus ponens (2, 4) (tautology #10)
(6) $\neg Q \to \neg P$ contrapositive of (a) (tautology #24)
(7) $\neg P$ modus ponens (5,6) (tautology #10)

We have proven that language P is not Turing-recognisable.