MT181 Number Systems: Answers to Revision Questions

For further questions and questions on congruences and relations see Sheet 10 and *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009), or the other books in the recommended reading.

You should also practice by doing past January Tests.

FUNCTIONS. Let X and Y be sets. Recall from Definitions 2.5 and 2.11 that a function $f : X \to Y$ is

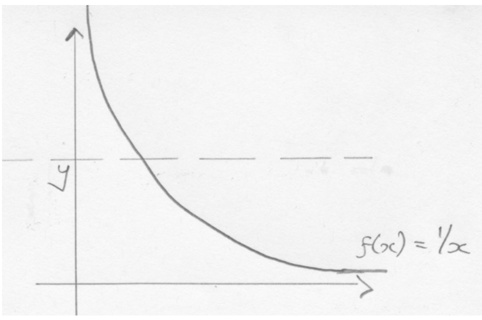
(i) *bijective* if for all $y \in Y$ there exists a unique x such that $f(x) = y$,
(ii) *injective* if $f(x) = f(x') \implies x = x'$,
(iii) *surjective* if for each $y \in Y$ there exists some $x \in X$ such that $f(x) = y$,

Equivalently

- f is injective if for all $y \in Y$ there exists at most one x such that $f(x) = y$,
- f is bijective if and only if f is injective and surjective.

You are welcome to use these as alternative definitions. **Definitions must be accurately stated to get marks in an exam.**

These properties can be recognized from the graph of a function. For example, let $\mathbb{R}^{>0} = \{x \in \mathbb{R} : x > 0\}$ and consider $f : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$ defined by $f(x) = 1/x$. The graph is shown below.

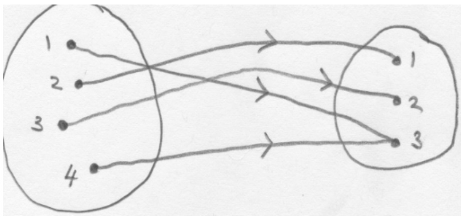


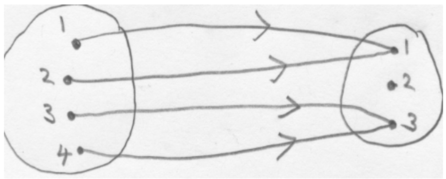
Since for each $y \in \mathbb{R}^{>0}$ the horizontal line of height y meets the graph at a unique point, the function is bijective.

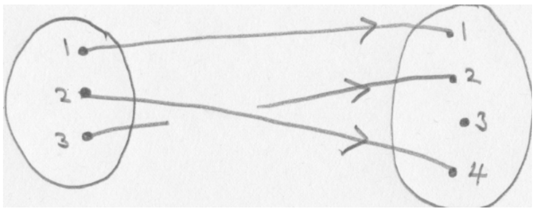
If instead we define $g : \mathbb{R}^{>0} \to \mathbb{R}$ by $g(x) = 1/x$ then g has the same graph as f, but g is no longer surjective. For instance, -1 is in the codomain of g and $g(x) \neq -1$ for any $x \in \mathbb{R}^{>0}$. Correspondingly, the horizontal line of height -1 does not meet the graph above.

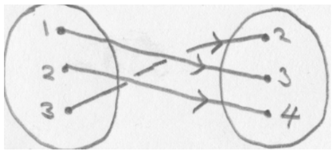
This underlines the point that when defining a function **it is essential to specify the domain and codomain**.

1. For each of the diagrams below decide whether the function it represents is (1) injective, (2) surjective, (3) bijective.









Top left:

(1) not injective since $f(1) = f(4) = 3$;
(2) surjective since for all $y \in \{1, 2, 3\}$ there exists $x \in \{1, 2, 3, 4\}$ such that $f(x) = y$ (specifically: $f(2) = 1$, $f(3) = 2$, $f(4) = 3$);
(3) not bijective, since not injective.

Top right:

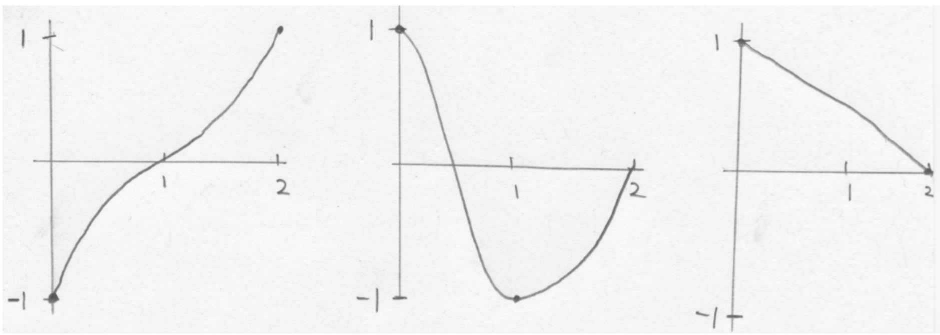
(1) not injective since $f(1) = f(2) = 1$;
(2) not surjective: there is no $x \in \{1, 2, 3, 4\}$ such that $f(x) = 2$;
(3) not bijective since not injective.

Bottom left:

(1) injective;
(2) not surjective: there is no $x \in \{1, 2, 3, 4\}$ such that $f(x) = 3$;
(3) not bijective since not surjective.

Bottom right: (1) injective; (2) surjective; (3) hence bijective.

2. Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 2\}$ and let $Y = \{y \in \mathbb{R} : -1 \leq y \leq 1\}$. The graphs below show three functions $f : X \to Y$. Decide for each each graph whether the function it shows is (1) injective, (2) surjective, (3) bijective.



Left function: (1) injective, (2) surjective and so (3) bijective.

Middle function:

(1) not injective: for example there exists $x < 1$ such that $f(x) = f(2) = 0$;
(2) surjective;
(3) not bijective since not injective.

Right function:

(1) injective;
(2) not surjective, for instance the horizontal line through $-1/2$ does not meet the graph so there is no $x \in [0, 2]$ such that $f(x) = -1/2$;
(3) not bijective since not surjective.

Exercise. Let X and Y be as above. Sketch the graph of a function $f : X \to Y$ that is neither injective nor surjective.

3. Let $X = \{x \in \mathbb{R} : x \neq -1\}$ and let $Y = \{y \in \mathbb{R} : y \neq 0\}$. Let $g : X \to Y$ be the function defined by

$$g(x) = \frac{1}{x+1}$$

Show that g is bijective and find a formula for $g^{-1} : Y \to X$.

Let $y \in Y$. We have

$$g(x) = y \iff \frac{1}{x+1} = y \iff x + 1 = \frac{1}{y} \iff x = \frac{1}{y} - 1$$

Since $1/y \neq 0$ we have $1/y - 1 \in X$. Hence for each $y \in Y$ there exists a unique $x \in X$ such that $g(x) = y$. Thus g is bijective and

$$g^{-1}(y) = \frac{1}{y} - 1$$

for all $y \in Y$.

Complex Numbers.

4. (a) Write $-1 - i$ in polar and exponential forms.

(b) Let $\phi = \tan^{-1} 2$. Plot $1+2i$, $2+i$, $-2+i$ and $-1-2i$ on an Argand diagram, and convert these numbers to polar form, writing your answers in terms of ϕ and multiples of π.

(c) Let $z = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. Write z in polar and exponential forms.

(d) What are $\mathrm{Arg}(i)$ and $\mathrm{Arg}(-i)$? Put i and $-i$ in exponential form.

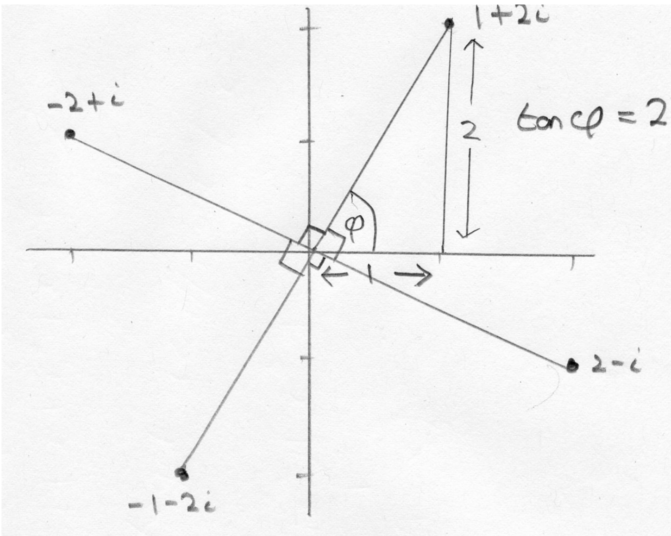
(e) Convert $\mathrm{e}^{-\pi i/6}$ to Cartesian form.

(a) Since $|-1-i| = \sqrt{(-1)^2+(-1)^2} = \sqrt{2}$ and $\mathrm{Arg}(-1-i) = \pi + \pi/4 = 5\pi/4$ we have

$$-1-i = \sqrt{2}(\cos 5\pi/4 + i\sin 5\pi/4) = \sqrt{2}\mathrm{e}^{i5\pi/4}.$$

It would also be entirely correct to write $-1-i = \sqrt{2}(\cos 3\pi/4 - i\sin 3\pi/4) = \sqrt{2}\mathrm{e}^{-i3\pi/4}$, using that $-3\pi/4$ is also an argument of $-1-i$.

(b) See the diagram below.



From this diagram we see that all the numbers have modulus $\sqrt{5}$ and that

$$\begin{aligned}
\mathrm{Arg}(1+2i) &= \phi \\
\mathrm{Arg}(-2+i) &= \phi + \pi/2 \\
\mathrm{Arg}(-1-2i) &= \phi + \pi \\
\mathrm{Arg}(2-i) &= \phi + 3\pi/2.
\end{aligned}$$

Hence

$$\begin{aligned}
1+2i &= \sqrt{5}\big(\cos\phi + i\sin\phi\big) \\
-2+i &= \sqrt{5}\big(\cos(\phi+\pi/2) + i\sin(\phi+\pi/2)\big) \\
-1-2i &= \sqrt{5}\big(\cos(\phi+\pi) + i\sin(\phi+\pi)\big) \\
2-i &= \sqrt{5}\big(\cos(\phi+3\pi/2) + i\sin(\phi+3\pi/2)\big).
\end{aligned}$$

Again you could give different (but equivalent) answers by taking a different choice for the argument. For example,

$$2-i = \sqrt{5}\big(\cos(\phi-\pi/2) + i\sin(\phi-\pi/2)\big).$$

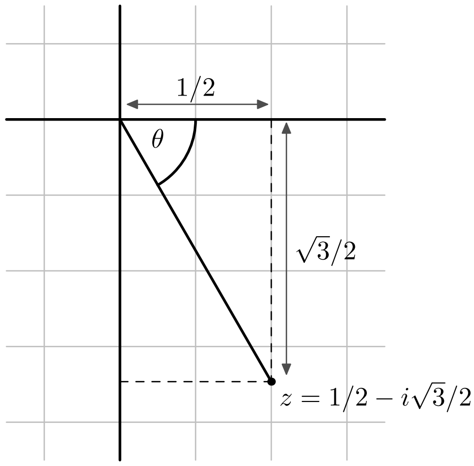
(c) $|z| = (\frac{1}{2})^2 + (\frac{-\sqrt{3}}{2})^2 = \frac{1}{4} + \frac{3}{4} = 1$. From the diagram below we see that z has argument $-\theta$ (negative since below the real axis) where

$$\tan\theta = \frac{\frac{\sqrt{3}}{2}}{\frac{1}{2}} = \sqrt{3}.$$

Hence $\theta = \pi/3$ and

$$z = \cos(\pi/3) - i\sin(\pi/3) = \mathrm{e}^{-i\pi/3}.$$

Note that the principal argument of z is $\mathrm{Arg}(z) = 2\pi - \pi/3 = 5\pi/3$, according to the definition given in lectures.

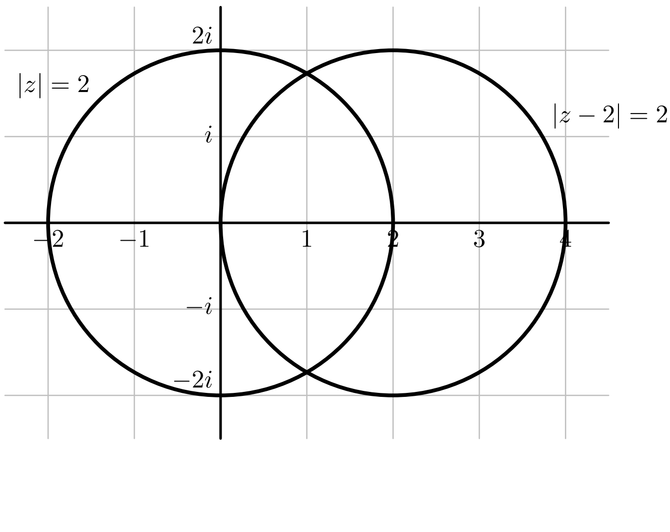


(d) $\mathrm{Arg}(i) = \pi/2$, $\mathrm{Arg}(-i) = 3\pi/2$, and $i = \mathrm{e}^{i\pi/2}$, $-i = \mathrm{e}^{3i\pi/2}$. You could also write $-i = \mathrm{e}^{-i\pi/2}$, but note that according to the definition given in lectures, the principal argument of $-i$ is $3\pi/2$.

(e) $\mathrm{e}^{-\pi i/6} = \cos\pi/6 - i\sin\pi/6 = \frac{\sqrt{3}}{2} - \frac{i}{2}$.

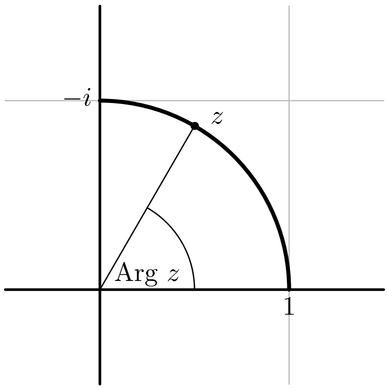
5. Draw the sets $\{z \in \mathbb{C} : |z| = 2\}$ and $\{w \in \mathbb{C} : |w - 2| = 2\}$ on the same Argand diagram.

We have $|z| = 2$ if and only if z is distance 2 from 0. So the first set is the circle of radius 2 about 0. The condition $|w - 2| = 2$ means that w is distance 2 from 2 on the Argand diagram. So the second set is a circle of radius 2 about 2.



6. Let T be the set of $z \in \mathbb{C}$ such that $|z| = 1$ and $0 \leq \operatorname{Arg} z \leq \pi/2$. Draw T on an Argand diagram.

The condition $|z| = 1$ means that z is on the unit circle; the condition $0 \leq \operatorname{Arg} z \leq \pi/2$ means that the marked angle θ is between 0 and $\pi/2$. Therefore we get the arc shown below.



7. Solve the following equations, giving the solutions in Cartesian form. Be sure to give all solutions.

(a) $(1+i)z - (3+i) = 6$,
(b) $(z+3)^3 = -2$,
(c) $\exp z = 10 + 10i$,
(d) $z + \bar{z} = 3$

(a) Since

$$(1+i)z-(3+i) = 6 \iff (1+i)z = 6+(3+i) \iff (1+i)z = 9+i \iff z = \frac{9+i}{1+i}$$

the unique solution is

$$z = \frac{9+i}{1+i} = \frac{(9+i)(1-i)}{(1+i)(1-i)} = \frac{9+i-9i+1}{2} = \frac{10-8i}{2} = 5-4i.$$

(b) Let $w = z+3$. If $w = re^{i\theta}$ then $w^3 = r^3 e^{3i\theta}$. So

$$\begin{aligned} w^3 = -2 &\iff r^3 e^{3i\theta} = 2e^{i\pi} \\ &\iff r^3 = 2 \text{ and } 3\theta = \pi + 2n\pi \text{ for some } n \in \mathbb{Z} \\ &\iff r = \sqrt[3]{2} \text{ and } \theta = \pi/3 + 2n\pi/3 \text{ for some } n \in \mathbb{Z}. \end{aligned}$$

Taking $\theta = \pi/3, \pi, 5\pi/3$ gives the three solutions

$$\begin{aligned} &\sqrt[3]{2}(\cos\pi/3 + i\sin\pi/3) = \sqrt[3]{2}\,\frac{1+i\sqrt{3}}{2} \\ &\sqrt[3]{2}(\cos\pi + i\sin\pi) = -\sqrt[3]{2} \\ &\sqrt[3]{2}(\cos 5\pi/3 + i\sin 5\pi/3) = \sqrt[3]{2}\,\frac{1-i\sqrt{3}}{2}. \end{aligned}$$

Taking further values for θ just repeats these solutions so there are no more. (For instance $5\pi/3 + 2\pi/3 = 7\pi/3 = 2\pi + \pi/3$, so taking $\theta = 7\pi/3$ just gives the first solution again.) Hence the solutions for z are

$$\frac{\sqrt[3]{2}}{2} - 3 + i\frac{\sqrt[3]{2}\sqrt{3}}{2}, \quad -\sqrt[3]{2} - 3, \quad \frac{\sqrt[3]{2}}{2} - 3 - i\frac{\sqrt[3]{2}\sqrt{3}}{2}$$

in Cartesian form.

(c) Let $z = a + bi$. Since $10 + 10i = 10\sqrt{2}(1+i) = 10\sqrt{2}\mathrm{e}^{i\pi/4}$ we have

$$\begin{aligned} \exp z = 10 + 10i &\iff \mathrm{e}^a\mathrm{e}^{bi} = 10\sqrt{2}\mathrm{e}^{i\pi/4} \\ &\iff \mathrm{e}^a = 10\sqrt{2} \text{ and } b = i\pi/4 + 2n\pi \text{ for some } n \in \mathbb{Z}. \end{aligned}$$

Therefore the solutions are

$$z = \ln 10 + \tfrac{1}{2}\ln 2 + i(\frac{\pi}{4} + 2n\pi)$$

for $n \in \mathbb{Z}$.

(d) Let $z = a + bi$. Then

$$z + \bar{z} = 3 \iff (a + bi) + (a - bi) = 3 \iff 2a = 3$$

so the solutions are $z = 3/2 + bi$ where b can be any real number.

Induction and natural numbers.

8. (a) Prove by induction that

$$\sum_{k=1}^{n} k^2 = \frac{1}{3}n(n + \tfrac{1}{2})(n+1)$$

for all $n \in \mathbb{N}$.

(b) Prove by induction (or using congruences if you prefer) that $7^n - 1$ is divisible by 6 for all $n \in \mathbb{N}$.

(c) Prove by induction that $1 + 1/2 + \cdots + 1/2^n = 2 - 1/2^n$ for all $n \in \mathbb{N}_0$.

(a) *Base case:* putting $n = 1$ we need $\sum_{k=1}^{1} k^2 = \frac{1}{3}1(1 + \frac{1}{2})(1+1)$. This is true since $1 = \frac{1}{3} \times \frac{3}{2} \times 2$. *Inductive step:* assume that $\sum_{k=1}^{n} k^2 =$

$\frac{1}{3}n(n+\frac{1}{2})(n+1)$. Then

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= \Big(\sum_{k=1}^{n} k^2\Big) + (n+1)^2 \\ &= \frac{1}{3}n(n+\tfrac{1}{2})(n+1) + (n+1)^2 \\ &= \frac{n+1}{3}\big(n(n+\tfrac{1}{2}) + 3(n+1)\big) \\ &= \frac{n+1}{3}(n^2 + \frac{7n}{2} + 3) \\ &= \frac{n+1}{3}(n+\tfrac{3}{2})(n+2) \\ &= \frac{(n+1)(n+1+\frac{1}{2})(n+1+1)}{3}\end{aligned}$$

as required.

(b) *Base case:* $7^1 - 1 = 6$ is clearly divisible by 6. *Inductive step:* suppose that $7^n - 1$ is divisible by 6. So $7^n - 1 = 6q$ for some $q \in \mathbb{Z}$. Hence

$$7^{n+1} - 1 = 7 \times 7^n - 1 = 7 \times (7^n - 1) + 6 = 7 \times 6q + 6 = 6(7q+1)$$

and so $7^{n+1} - 1$ is a multiple of 6.

Alternative: using congruences, we can simply argue that $7 \equiv 1 \bmod 6$ so $7^n - 1 \equiv 1^n - 1 \equiv 0 \bmod 6$.

(c) *Base case:* Here the base case is when $n = 0$, since we are asked to prove the statement for all $n \in \mathbb{N}_0$. We need $1 = 2 - 1/2^0$ and clearly this is true. *Inductive step:* assume that $1 + 1/2 + \cdots + 1/2^n = 2 - 1/2^n$. Then

$$1 + 1/2 + \cdots + 1/2^n + 1/2^{n+1} = 2 - 1/2^n + 1/2^{n+1} = 2 - 1/2^{n+1}$$

as required.

9. Work through Euclid's proof that there are infinitely many primes. Then, a day later, try to write out your own version of the proof, or explain it to a friend.

Probably a useful exercise, but of no value unless you do it yourself. You could also listen to Dr Vicky Neale explain the proof `http://www.bbc.co.uk/podcasts/series/historyofideas#playepisode8`.

10. (a) Express 79 in base 2.

(b) Let $0 \le a, b, c \le 9$. Show that the base 10 number $abccba$ is divisible by 11.

(c) Let $0 \le a_k \le 9$ for each $k \in \{0, 1, \dots, d-1\}$. Prove that

$$\sum_{k=0}^{d-1} a_k 10^k \text{ is divisible by } 9 \iff \sum_{k=0}^{d-1} a_k \text{ is divisible by } 9.$$

[*Hint:* this may be easiest to do using congruences moduo 9.]

(d) Is 123456789987654321 a multiple of 9?

(a) Since $79 = 64 + 8 + 4 + 2 + 1$, in binary we have $79 = 1001111_2$. Or you could use the repeated division algorithm:

$$\begin{aligned} 79 &= 2 \times 38 + 1 \\ 38 &= 2 \times 19 + 1 \\ 19 &= 2 \times 9 + 1 \\ 9 &= 2 \times 4 + 1 \\ 4 &= 2 \times 2 + 0 \\ 2 &= 2 \times 1 + 0 \\ 1 &= 0 \times 2 + 1, \end{aligned}$$

reading the sequence of remainders from bottom to top to get 1001111.

(b) By definition $abccba = 100000a + 10000b + 1000c + 100c + 10b + a = 100001a + 10010b + 1100c$. Now $100001 = 11 \times 9091$ and $10010 = 11 \times 910$ and $1100 = 11 \times 100$, so

$$abccba = 11 \times 9091a + 11 \times 910b + 11 \times 100c = 11 \times (9091a + 910b + 100c).$$

Hence $abccba$ is divisible by 11.

(c) Since $10^k - 1 = 9 \dots 9 = 9 \times 1 \dots 1$ (with k nines and k ones), $10^k - 1$ is divisible by 9. So

$$\sum_{k=0}^{d-1} a_k 10^k = \sum_{k=0}^{d-1} a_k (10^k - 1) + \sum_{k=0}^{d-1} a_k$$

where every summand in the first sum is divisible by 9. So

$$\sum_{k=0}^{d-1} a_k 10^k = 9q + \sum_{k=0}^{d-1} a_k$$

for some $q \in \mathbb{Z}$ and $\sum_{k=0}^{d-1} a_k 10^k$ is divisible by 9 if and only if $\sum_{k=0}^{d-1} a_k$ is divisible by 9.

Alternative: since $10 \equiv 1 \bmod 9$ we have

$$\sum_{k=0}^{d-1} a_k 10^k \equiv \sum_{k=0}^{d-1} a_k 1^k \equiv \sum_{k=0}^{d-1} a_k \bmod 9.$$

Now use that n is divisible by 9 if and only if $n \equiv 0 \bmod 9$.

(d) Yes, 123456789987654321 is a multiple of 9 since its sum of digits is $2 \times 9 \times 10/2 = 90$ and $90 = 9 \times 10$.

PROPOSITIONS.

11. Show that the following propositions formed from propositions P, Q and R are logically equivalent:

(a) $(P \implies Q)$ and $(\neg Q \implies \neg P)$,
(b) $\neg(P \vee Q \vee R)$ and $\neg P \wedge \neg Q \wedge \neg R$,
(c) $P \implies (Q \vee R)$ and $\neg P \vee Q \vee R$.

(a) Suppose $P \implies Q$ is true. If $\neg Q$ is true then P cannot be true (since from $P \implies Q$ we get that Q is true). Hence $\neg P$ is true. So $(P \implies Q) \implies (\neg Q \implies \neg P)$. Now set $P = \neg Q'$ and $Q = \neg P'$ to get

$$(\neg Q' \implies \neg P') \implies (\neg\neg P' \implies \neg\neg Q').$$

Since P' is logically equivalent to $\neg\neg P'$, this implies

$$(\neg Q' \implies \neg P') \implies (P' \implies Q').$$

Now erase the primes to get the result.

Alternatives: a direct proof that $(\neg Q \implies \neg P) \implies (P \implies Q)$, along the lines of the proof that $(P \implies Q) \implies (\neg Q \implies \neg P)$ above, was given in lectures. Or you can just use truth tables.

(b) $\neg(P \vee Q \vee R)$ is true $\iff$ $P \vee Q \vee R$ is false $\iff$ P, Q and R are all false. Similarly $\neg P \wedge \neg Q \neg R$ is true $\iff$ $\neg P$, $\neg Q$, $\neg R$ are all true $\iff$ P, Q and R are all false. Hence the propositions are logically equivalent.

(c) $P \implies A$ is logically equivalent to $\neg P \vee A$. Hence

$$P \implies (Q \vee R) \iff \neg P \vee (Q \vee R) \iff \neg P \vee Q \vee R.$$

Or you could observe that the columns for $P \implies (Q \vee R)$ and $\neg P \vee Q \vee R$ in the truth table below are the same.

P	Q	R	$Q \vee R$	$P \implies (Q \vee R)$	$\neg P \vee Q \vee R$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	T	T	T
T	F	F	F	F	F
F	T	T	T	T	T
F	T	F	T	T	T
F	F	T	T	T	T
F	F	F	F	T	T

12. Negate each of the following propositions. Decide which are true and which are false. Justify your answers.

(a) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y^2 = x)$
(b) $(\forall x \geq 0)(\exists y \in \mathbb{R})(y^2 = x)$
(c) $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(n \geq x)$
(d) $(\exists n \in \mathbb{N})(\forall x \in \mathbb{R})(n \geq x)$

Following the rules for negation on page 45 of the printed lecture notes gives the following negations.

(a) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(y^2 \neq x)$
(b) $(\exists x \geq 0)(\forall y \in \mathbb{R})(y^2 \neq x)$
(c) $(\exists x \in \mathbb{R})(\exists n \in \mathbb{N})(n < x)$
(d) $(\forall n \in \mathbb{N})(\exists x \in \mathbb{R})(n < x)$

Now

(a) is false (and its negation is true) since $-1 \in \mathbb{R}$ and for all $y \in \mathbb{R}$, we have $y^2 \neq -1$.
(b) is true, since given $x \geq 0$ we can take $y = \sqrt{x}$ and $y^2 = x$.
(c) is true: given $x \in \mathbb{R}$ take $n = \lfloor x \rfloor + 1$.
(d) The negation of (d) is true, since given $n \in \mathbb{N}$, we can take $x = n + 1$ and then $n < x$. Hence (d) is false.

13. Which of the following are tautologies? Justify your answers. (If you use truth tables, make it clear which feature of the truth table you use.)

(a) $(P \iff Q) \iff \big((P \wedge Q) \vee (\neg P \wedge \neg Q)\big)$,
(b) $(P \implies Q) \implies (Q \implies P)$,
(c) $\big(P \implies (Q \implies R)\big) \implies \big(Q \implies (P \implies R)\big)$.

(a) is a tautology since $P \iff Q$ is true if and only if P and Q are either both true or both false, so if and only if either $P \wedge Q$ or $\neg P \wedge \neg Q$ is true. Or you could use the truth table below, where A stands for $\big((P \wedge Q) \vee (\neg P \wedge \neg Q)\big)$, observing that the columns for $P \iff Q$ and A are the same.

P	Q	$P \iff Q$	$P \wedge Q$	$\neg P \wedge \neg Q$	A
T	T	T	T	F	T
T	F	F	F	F	F
F	T	F	F	F	F
F	F	T	F	T	T

(b) is not a tautology, since if P is false and Q is true then $P \Longrightarrow Q$ is true, and $Q \Longrightarrow P$ is false, and so $(P \Longrightarrow Q) \Longrightarrow (Q \Longrightarrow P)$ is false.

Remark. People who think that $P \Longrightarrow Q$ implies $Q \Longrightarrow P$ are commiting the logical fallacy of thinking a statement implies its converse. Here, once again, is the lottery example:

'If a person has won the lottery (P) then he or she is rich (Q).'

This does not imply

'If a person is rich (Q) then he or she has won the lottery (P).'

(c) Since $A \Longrightarrow B$ is false if and only if A is true and B is false, the proposition is false if and only if $Q \Longrightarrow (P \Longrightarrow R)$ is false and $P \Longrightarrow (Q \Longrightarrow R)$ is true. So we need Q to be true and $P \Longrightarrow R$ to be false, so P and Q are true and R is false. But then $(Q \Longrightarrow R)$ is false, so $P \Longrightarrow (Q \Longrightarrow R)$ is false.

Alternative. Let C be the proposition in (c). The final column of the truth table below shows that C is always true.

P	Q	R	$Q \Longrightarrow R$	$P \Longrightarrow (Q \Longrightarrow R)$	$P \Longrightarrow R$	$Q \Longrightarrow (P \Longrightarrow R)$	C
T	T	T	T	T	T	T	T
T	T	F	F	F	F	F	T
T	F	T	T	T	T	T	T
T	F	F	T	T	F	T	T
F	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Sets.

14. Let X be the set $\{1, \pi, \{42, \sqrt{2}\}, \{\{1,3\}\}\}$. Decide which of the following statements are true and which are false.

(i) $\pi \in X$;
(ii) $\{\pi\} \notin X$;
(iii) $\{42, \sqrt{2}\} \in X$;
(iv) $\{1\} \subseteq X$;
(v) $\{1, \sqrt{2}\} \subseteq X$;
(vi) $\{1, \pi\} \subseteq X$;
(vii) $(\exists A \in X)(1 \in A)$;
(viii) $\{1,3\} \subseteq X$;
(ix) $\{1,3\} \in X$
(x) $(\exists A \in X)(\{1,3\} \in A)$;

(i) True, (ii) True, (iii) True, (iv) True, (v) False: $\sqrt{2} \notin X$, (vi) True, (vii) False: no element of X has 1 as an element, (viii) False: $3 \notin X$, (ix) False, (x) True: take $A = \{\{1,3\}\} \in X$.

15. Define subsets X, Y and Z of the natural numbers as follows:

$$X = \{n \in \mathbb{N} : 6 \text{ divides } n-1\}$$
$$Y = \{n \in \mathbb{N} : 3 \text{ divides } n-1\}$$
$$Z = \{n \in \mathbb{N} : 3 \text{ divides } n^2-1.\}$$

(a) Let $n \in \mathbb{N}$. Show that $n \in X \implies n \in Y$.
(b) Is $X \subseteq Y$ true? Is $Y \subseteq X$ true?
(c) Let $n \in \mathbb{N}$. Show that $n \in Y \implies n \in Z$.
(d) Is $X \subseteq Z$ true?

(a) We use a chain of implications:

$$\begin{aligned} n \in X &\implies 6 \text{ divides } n-1 \\ &\implies (\exists q \in \mathbb{Z})(n-1 = 6q) \\ &\implies (\exists s \in \mathbb{Z})(n-1 = 3s) \quad ; \text{take } s = 2q \\ &\implies 3 \text{ divides } n-1 \\ &\implies n \in Y. \end{aligned}$$

(b) Since $n \in X \implies n \in Y$ we have $X \subseteq Y$. Since $4 \in Y$ but $4 \notin X$, $Y \not\subseteq X$.

(c) We have

$$\begin{aligned} n \in Y &\implies 3 \text{ divides } n-1 \\ &\implies (\exists q \in \mathbb{Z})(n-1 = 3q) \\ &\implies (\exists s \in \mathbb{Z})\big((n-1)(n+1) = 3s) \quad ; \text{take } s = (n+1)q \\ &\implies (\exists s \in \mathbb{Z})(n^2-1 = 3s) \\ &\implies 3 \text{ divides } n^2-1 \\ &\implies n \in Z. \end{aligned}$$

(d) Since $X \subseteq Y$ and $Y \subseteq Z$, we have $X \subseteq Z$.

Remark. The answer to (d) uses the transitivity of the $\subseteq$ relation. There is a corresponding transitivity of implication: $(P \implies Q) \wedge (Q \implies R)$ implies $P \implies R$.