1. (**5 marks**) Let $f : \mathbb{N} \to A$ be defined by $f(n) = 2 - \frac{1}{2^n}$. Then $2 - \frac{1}{2^m} = 2 - \frac{1}{2^n} \iff \frac{1}{2^m} = \frac{1}{2^n} \iff 2^n = 2^m \iff m = n$. Also for all $y \in A, y = 2 - \frac{1}{2^n}, n \in \mathbb{N}$, so f a bijection. Furthermore $m \leq n \implies 2^m \leq 2^n \implies \frac{1}{2^m} \geq \frac{1}{2^n} \implies 2 - \frac{1}{2^m} \leq 2 - \frac{1}{2^n}$ so this is a po isomorphism.

2. (**6 marks**) Suppose first that F is not 1-1. We must show that f is not 1-1, so there exist $P, Q \subseteq A, P \neq Q$ with $F(P) = F(Q)$. $P \neq Q \implies (\exists x \in P \setminus Q)) \vee (\exists x \in Q \setminus P)$. Suppose without loss of generality that $x \in P \setminus Q$. Then since $F(P) = F(Q), \exists y \in Q : f(y) = f(x) \in F(p) = F(Q)$. So $\exists y \in Q : f(y) = f(x)$ but $x \neq y$ since $x \in Q^{\complement}$ and $y \in Q$. Hence f is not 1-1.

Conversely if f is not 1-1 $\exists x, y : x \neq y$ such that $f(x) = f(y)$. Then $F(\{x\}) = F(\{y\}) = f(x) = f(y)$ but $\{x\} \neq \{y\}$ so F not 1-1.

3. (**7 marks**) Suppose $g \circ f$ is one-to-one and f is onto. Let $x, y \in B$ with $g(x) = g(y)$. Since f is onto, there exist $a, b \in A$ with $f(a) = x$ and $f(b) = y$. Then $g(f(a)) = g(x) = g(y) = g(f(b))$, i.e. $(g \circ f)(a) = (g \circ f)(b)$, so since $g \circ f$ is one-to-one we have $a = b$, so $f(a) = f(b)$, i.e. $x = y$.

4. (**4+4+7+4+3=22 marks**) We use the rules $x \in f^{-1}(T) \iff f(x) \in T$, $x \in \bigcap_{\alpha \in \Lambda} T_\alpha \iff (\forall \alpha \in \Lambda)(x \in T_\alpha)$ and $x \in \bigcup_{\alpha \in \Lambda} T_\alpha \iff (\exists \alpha \in \Lambda)(x \in T_\alpha)$.

(a) $x \in f^{-1}(S_Y^{\complement}) \iff f(x) \in (S_Y^{\complement}) \iff f(x) \notin S \iff x \notin f^{-1}(S) \iff x \in f^{-1}(S)_X^{\complement}$.

(b) $x \in f^{-1}(A \setminus B) \iff f(x) \in A \setminus B \iff f(x) \in A \cap B^{\complement} \iff (f(x) \in A) \wedge (f(x) \in B^{\complement} \iff (x \in f^{-1}(A)) \wedge (x \in f^{-1}(B^{\complement})) \iff x \in f^{-1}(A) \cap (f^{-1}B)^{\complement} \iff x \in f^{-1}(A) \setminus f^{-1}(B)$.

(c) We have

$$\begin{aligned}
x \in f^{-1}(A \setminus \bigcap_{\alpha \in \Lambda} S_\alpha) &\iff f(x) \in A \setminus \bigcap_{\alpha \in \Lambda} S_\alpha \\
&\iff (f(x) \in A) \wedge \sim((\forall \alpha \in \Lambda)(f(x) \in S_\alpha)) \\
&\iff (f(x) \in A) \wedge (\exists \alpha \in \Lambda) \sim(f(x) \in S_\alpha)) \\
&\iff (\exists \alpha \in \Lambda)(f(x) \in A) \wedge (f(x) \notin S_\alpha)) \\
&\iff (\exists \alpha \in \Lambda)(x \in f^{-1}A) \wedge (x \notin f^{-1}S_\alpha)) \\
&\iff (\exists \alpha \in \Lambda)(x \in f^{-1}A \setminus f^{-1}S_\alpha) \\
&\iff (\exists \alpha \in \Lambda)(x \in f^{-1}(A \setminus S_\alpha)) \\
&\iff x \in \bigcup_{\alpha \in \Lambda} f^{-1}(A \setminus S_\alpha)
\end{aligned}$$

so $f^{-1}(A \setminus \bigcap_{\alpha \in \Lambda} S_\alpha) = \bigcup_{\alpha \in \Lambda} f^{-1}(A \setminus S_\alpha)$.

(d) $x \in f(A) \setminus f(B) \implies (x \in f(A)) \wedge (x \notin f(B))$. Hence $x = f(p)$ for some $p \in A$ but there does not exist $q \in B : x = f(q)$. Hence $p \in A$ but $p \notin B$. so $p \in A \setminus B$ and hence $x = f(p) \in f(A \setminus B)$. Hence $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

(e) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Then$f(\mathbb{R} \setminus (-\infty, 0)) = f([0, \infty) = [0, \infty)$ but $f(\mathbb{R}) \setminus f(-\infty, 0) = [0, \infty) \setminus (0, \infty) = \{0\}$.

5. (**4x3=12 marks**) There exists such $x = b + (-a)$, as in the notes since then $a + x = a + (b + (-a)) = a + ((-a) + b) = (a + (-a)) + b) = 0 + b = b$. Moreover x is unique, since if $a + y = b$ then $y = 0 + y = (a + (-a)) + y = a + ((-a) + y) = a + (y + (-a)) = (a + y) + (-a) = b + (-a) = x$.

(a) Let $x \in \mathbb{Z}$. Then we have

$$\begin{aligned} (-x) + x &= x + (-x) && \text{(commutative law)} \\ &= 0 && \text{(definition of } -x\text{)} \end{aligned}$$

so by definition of $-(-x)$, $-(-x) = x$.

(b) Let $x \in \mathbb{Z}$. Then we have

$$\begin{aligned} x + (-1) \cdot x &= 1 \cdot x + (-1) \cdot x && \text{(definition of 1)} \\ &= x \cdot 1 + x \cdot (-1) && \text{(commutative law)} \\ &= x \cdot (1 + (-1)) && \text{(distributive law)} \\ &= x \cdot 0 && \text{(definition of } -1\text{)} \\ &= 0 \cdot x && \text{(commutative law)} \\ &= 0. && \text{(proved in lectures)} \end{aligned}$$

$$\begin{aligned} x \cdot (y - z) &= x \cdot (y + (-z)) && \text{(definition of "-")} \\ &= x \cdot y + x \cdot (-z) && \text{(distributive law)} \\ &= x \cdot y + -(x \cdot z) \\ &= x \cdot y - x \cdot z && \text{(definition of "-")} \end{aligned}$$

Hence, by definition of $-x$, $-x = (-1) \cdot x$.

6. (**3x3=9 marks**)

(a) The algorithm gives us

n	x	y	
78	1	0	r_1
72	0	1	r_2
6	1	-1	$r_3 = r_1 - r_2$
0	-12	13	$r_4 = r_3 - 12r_2$

From which we see that $\gcd(78, 72) = 6$ and $6 = 78 \cdot (1) + 72 \cdot (-1)$.

(b) The algorithm gives us

n	x	y	
2944	1	0	r_1
928	0	1	r_2
160	1	-3	$r_3 = r_1 - 3r_2$
128	-5	16	$r_4 = r_2 - 5r_3$
32	6	-19	$r_5 = r_3 - r_4$
0	-29	92	$r_5 = r_3 - 4r_4$

From this we see that $\gcd(2944, 928) = 32 = 2944 \cdot (6) + 928 \cdot (-19)$.

(c) The algorithm gives us

n	x	y	
1173	1	0	r_1
957	0	1	r_2
216	1	-1	$r_3 = r_1 - r_2$
93	-4	5	$r_4 = r_2 - 2r_3$
30	9	-11	$r_5 = r_3 - 2r_4$
3	-31	38	$r_5 = r_3 - 3r_4$
0	319	-391	$r_5 = r_3 - 10r_4$

from which we see that $\gcd(1173, 957) = 3$ and $3 = 1173 \cdot (-23) + 957 \cdot 33$.

7. (**3 marks**) Suppose that $a, b, c, x, y \in \mathbb{Z}$ with $c \mid a$ and $c \mid b$. Then there exist $p, q \in \mathbb{Z}$ with $a = cp$ and $b = cq$. But then

$$ax + by = (cp)x + (cq)y = c(px + qy),$$

and $(px + qy) \in \mathbb{Z}$, so $c \mid ax + by$ as required.

8. (**16 marks**)

(a) Suppose there exist $x, y \in \mathbb{Z}$ with $rx + sy = 1$. Put $d = \gcd(r, s)$. Then, by the previous question, $d \mid 1$, so $d = 1$. So r and s are relatively prime.

(b) Suppose that s and $r - s$ are not relatively prime. Then there is some $d > 1$ such that $d \mid s$ and $d \mid r - s$. But then, by the previous question, $d \mid s \cdot (1) + (r - s) \cdot 1$, i.e. $d \mid r$. Thus d is a common divisor of r and s, so r and s are not relatively prime. Hence, by contraposition, if r and s are relatively prime then so are s and $r - s$.

(c) Let $c \in \mathbb{N}$ and suppose $c = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t}$, where each $\gamma_i \geq 0$. Then

$$\begin{aligned} ac = b \quad &\iff \quad p_1^{\alpha_1+\gamma_1} p_2^{\alpha_2+\gamma_2} \ldots p_t^{\alpha_t+\gamma_t} = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t} \\ &\iff \quad \alpha_i + \gamma_i = \beta_i \qquad \text{by the uniqueness of the fundamental theorem of arithmetic.} \end{aligned}$$

Thus $a \mid b \iff \alpha_i \leq \beta_i$.
Let $d = p_1^{m_1} p_2^{m_2} \ldots p_t^{m_t}$ and $D = \{x \in \mathbb{N} : x \mid a \ \wedge \ x \mid b\}$. Then $m_1 = \min\{\alpha_i, \beta_i\} \leq \alpha_i$, and by the above argument, $d \mid a$. Similarly, $d \mid b$ and $d \in D$.
Let $c = p_1^{\eta_1} p_2^{\eta_2} \ldots p_t^{\eta_t} \in D$. Then $c \mid a$ and by (a) again, each $\eta_i \leq \alpha_i$. Similarly, each $\eta_i \leq \beta_i$, so that $\eta_i \leq m_i$ and $c \mid d$. In particular, $c \leq d$ and $d = \gcd(a, b)$.

(d) We know from the notes theorem 20 (week 6) that if p is prime and $p \mid a \cdot b$ then $p \mid a$ or $p \mid b$. Hence P(2) is true. So we assume $p \mid m_1 m_2 \cdots m_k$ then $p \mid m_i$ for some i and consider $p \mid m_1 m_2 \cdots m_{k+1}$. Let $a = m_1 m_2 \cdots m_k$ then $p \mid a \vee p \mid m_{k+1}$, so $(\exists i \leq k : p \mid m_i) \vee (p \mid m_{k+1})$, so $p \mid m_i$ some $1 \leq i \leq k+1$. QED.