1. Let $v : \mathbb{Q}^\times \to \mathbb{Z}$ be a valuation. We first observe that $v(n) \geq 0$ for all integers $n \neq 0$. Indeed, we have $v(1) = 0$ since v is a homomorphism, and also $v(-1) = 0$ since $2v(-1) = v((-1)^2) = v(1) = 0$. If $n \in \mathbb{N}$ then $v(n) = v(1 + \cdots + 1) \geq 0$ (by the second axiom defining a valuation).

   There exists $a \in \mathbb{N}$ such that $v(a) > 0$. Otherwise we would have $v(a) = 0$ for all $a \in \mathbb{Z} - \{0\}$, hence for all $a \in \mathbb{Q}^\times$. Let us write $a = \prod_{i=1}^k p_i^{n_i}$ where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k \in \mathbb{N}$. Then $v(a) = \sum_{i=1}^k n_i v(p_i)$, so we can assume, after relabelling, that $v(p_1) > 0$. We will show that $v = v_{p_1}$. It is enough to show that $v(q) = 0$ for any prime $q \neq p_1$ (as then $v(p_1) = 1$ is forced by the surjectivity of v).

   Let $q \neq p_1$ be any prime. We can write (by Bezout's theorem) $rp_1 + sq = 1$ for some $r, s \in \mathbb{Z}$, hence $0 = v(1) = v(rp_1 + sq) \geq \min(v(p_1), v(q)) \geq 0$. This forces $v(q) = 0$.

2. The ring $\mathbb{Z}[X]$ is Noetherian (Hilbert basis theorem) and integrally closed (it is a UFD). However, not every non-zero prime is maximal: for example, the ideal (X) is not (its quotient is a domain, but not a field).

   The ring $R = \cup_{n \geq 1} \mathbb{C}[X^{1/n}]$ is integrally closed, and every non-zero prime ideal is maximal. Indeed, if $P \subset R$ is a non-zero prime ideal then there exists $N \geq 1$ such that $P_N = P \cap \mathbb{C}[X^{1/N}]$ is non-zero, and then $\mathbb{C}[X^{1/N}]/P_N = \mathbb{C}$. For any n divisible by N, $\mathbb{C}[X^{1/n}]/P_n$ is a domain which is a finite $\mathbb{C}$-module, which must therefore equal $\mathbb{C}$. We see that $R/P = \mathbb{C}$ and in particular is a field, hence P is a maximal ideal. However, R is not Noetherian: the sequence $(X) \subset (X^{1/2}) \subset (X^{1/4}) \subset \ldots$ of ideals is not eventually stationary.

   The ring $A = \mathbb{C}[t^2, t^3]$ is Noetherian (it is isomorphic to $\mathbb{C}[x, y]/(y^2 - x^3)$, so this follows from the Hilbert basis theorem), and every non-zero prime ideal is maximal: if P is a non-zero prime ideal, then either P contains t^2 (in which case $P = (t^2, t^3)$ and is maximal) or P does not contain t^2, in which case A_P is a localization of $\mathbb{C}[t^2, t^3][t^{-1}] = \mathbb{C}[t, t^{-1}]$. This latter ring is a PID, hence a Dedekind domain, showing that A_P is also a Dedekind domain and particular PA_P is a maximal ideal of A_P and hence P is a maximal ideal of A. However, A is not integrally closed as $t \in \operatorname{Frac} A$ is integral over A (it satisfies the equation $X^2 - t$).

3. Omitted - see Atiyah–Macdonald, Proposition 1.10.

4. (a) By unique factorization, it suffices to show that each non-zero prime ideal $P \subset R$ is principal. Let $P = P_1, \ldots, P_r$ be all the

distinct non-zero prime ideals of R. By the Chinese remainder theorem, we can find $a \in R$ such that $a \in P - P^2$ but $a \notin P_i$ for each $i = 2, \dots, r$. Then the ideal (a) satisfies $(a) \subset P$, $(a) \not\subset P^2$, and $a \not\subset P_i$ for each $i = 2, \dots, r$. In other words, $v_P(a) = 1$ and $v_{P_i}(a) = 0$ $(i = 2, \dots, r)$. This implies that $(a) = P$ and P is principal.

(b) Let $I \subset R$ be a non-zero ideal, and let $a \in I - \{0\}$. Then $(a) \subset I$, and hence $(a) = IJ$ for some non-zero ideal $J \subset R$. By the Chinese remainder theorem, we can find an element $b \in R$ such that $v_P(b) = v_P(I)$ if P is a non-zero prime of R such that $v_P(a) > 0$. We claim that $v_P((a, b)) = v_P(I)$ for all non-zero prime ideals $P \subset R$, which will imply that $(a, b) = I$.

To see this, note that $v_P((a, b)) = \min(v_P(a), v_P(b))$ (equality, not just inequality!). By construction, for all P we have $v_P(a) \geq v_P(I)$ and $v_P(b) = v_P(I)$ if $v_P(a) > 0$. This is enough.

5. We must show that the coefficients of $g_1(X), g_2(X)$ lie in A. Gauss' lemma shows that the coefficients lie in A_P for all non-zero prime ideals P. We have seen in lectures that $\cap_P A_P = A$, so the result follows.

6. If $M = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct primes and $a_1, \dots, a_k \in \mathbb{N}$, then each quotient $\mathbb{Z}/M^i\mathbb{Z} \cong \prod_{j=1}^k \mathbb{Z}/p_j^{ia_j}\mathbb{Z}$, by the Chinese remainder theorem. Inverse limits respect products, so we get an isomorphism

$$\varprojlim_i \mathbb{Z}/M^i\mathbb{Z} \cong \prod_{j=1}^{k} \varprojlim_i \mathbb{Z}/p_j^{ia_j}\mathbb{Z}.$$

We need to explain why there is an isomorphism

$$\varprojlim_i \mathbb{Z}/p_j^{ia_j}\mathbb{Z} \cong \varprojlim \mathbb{Z}/p_j^i\mathbb{Z} = \mathbb{Z}_{p_j}.$$

More generally, suppose given an inverse system (of groups say)

$$A_1 \leftarrow A_2 \leftarrow A_3 \leftarrow \dots$$

and an increasing sequence $j_1 < j_2 < j_3 < \dots$ of natural numbers. Define $B_i = A_{j_i}$. Then there is an inverse system

$$B_1 \leftarrow B_2 \leftarrow B_3 \leftarrow \dots$$

and a canonical isomorphism

$$\varprojlim_i A_i \to \varprojlim_i B_i,$$

which sends a sequence $(a_i)_{i\geq 1} \in \varprojlim_i A_i$ to the sequence $(b_i)_{i\geq 1} \in \varprojlim_i B_i$ defined by $b_i = a_{j_i}$.

7. We first show that if $x \in \mathbb{Q}_p$ has an eventually periodic p-adic expansion, then x is rational. We are free to multiply by powers of p, so we can assume that $x = \sum_{i=0}^\infty a_i p^i$ and $a_0 \neq 0$. We are also free to add and subtract numbers of the form $\sum_{i=0}^k a_i p^i$ (i.e. positive integers), so we assume that the p-adic expansion of x is periodic on the nose, say $a_{i+k} = a_i$ for all $i \geq 0$ and a fixed period $k > 0$.

   In this case we can write $x = (a_0+a_1p+\cdots+a_{k-1}p^{k-1})(1+p^k+p^{2k}+\dots)$. Noting that $1/(1-p^k) = \sum_{i=0}^\infty p^{ik}$, we see that $x \in \mathbb{Q}$.

   Now suppose conversely that $x \in \mathbb{Q}$; we will show that the p-adic expansion of x is eventually periodic. We first note that x has an eventually periodic expansion if and only if $-x$ does. Indeed, if $x = \sum_{i=0}^\infty a_j p^j$, and $a_0 \neq 0$, then $-x = (p - a_0) + \sum_{i=1}^\infty (p-1-a_j)p^j$. It follows that any integer has an eventually periodic p-adic expansion. We also note that multiplying by powers of p only shifts digits, so we can assume that $v_p(x) \geq 0$.

   Suppose that $x \in (-1, 0)$ and $v_p(x) \geq 0$. After multiplying by a negative power of p, we can assume further that $v_p(x) = 0$. Let us write $x = -a/b$, where a, b are positive coprime integers. Choose $k \geq 1$ such that $p^k \equiv 1 \bmod b$; then we can write $p^k - 1 = bc$, hence $x = -ac/bc = ac/(1-p^k) = \sum_{i=0}^\infty acp^{ik}$. Since $-x < 1$ we have $ac < p^k - 1$, hence we can write $ac = \sum_{j=0}^{k-1} a_j p^j$ for $a_j \in \{0, \dots, p-1\}$, and $x = \sum_{i,j\geq 0} a_j p^{j+ik}$ has a periodic expansion.

   Now suppose that $x < -1$, $v_p(x) \geq 0$, and $x \notin \mathbb{Z}$. Thus we can find $N \in \mathbb{N}$ such that $-(N+1) < x < -N$, hence $x + N \in (-1, 0)$ and we can apply the previous paragraph to write $x + N = \sum_{j=0}^\infty a_j p^j$. Infinitely many of the a_j are non-zero (as otherwise $x + N$ would be an integer), so we can find n such that $a_0 + a_1 p + \cdots + a_n p^n > N$, hence $x = (a_0 + a_1 p + \cdots + a_n p^n - N) + \sum_{j=n+1}^\infty a_j p^j$. We can write $a_0 + a_1 p + \cdots + a_n p^n - N = b_0 + b_1 p + \cdots + b_n p^n$, so the p-adic expansion of x is eventually periodic.

8. Define a map $\mathbb{Z}_p \to [0, 1]$ by sending $\sum_{i=0}^\infty a_i p^i$ to $\sum_{i=0}^\infty a_i p^{-(i+1)}$ (where the first sum is convergent in the p-adic topology, and the second sum in the real topology). This is continuous.

   There is no continuous surjection $[0, 1] \to \mathbb{Z}_p$. If there was, then $\mathbb{Z}_p$ would be connected, but it is not: $\mathbb{Z}_p = \mathbb{Z}_p^\times \sqcup (p)$ is a decomposition into disjoint open subsets.

9. Let $v : \mathbb{Q}_p^\times \to \mathbb{Z}$ be the p-adic valuation. We first note that if $(a_i)_{i \geq 1}$ is a sequence of elements in $\mathbb{Q}_p^\times$, then the sum $\sum_{i=1}^\infty a_i$ converges in $\mathbb{Q}_p$ if and only if $v(a_i) \to \infty$ as $i \to \infty$.

   Therefore the sum $1 + \sum_{n=1}^\infty x^n/n!$ converges if and only if $v(x^n/n!) = nv(x) - v(n!)$ tends to infinity as $n \to \infty$. We have

   $$v(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots.$$

   This gives an upper bound of

   $$v(n!) \leq n/p(1 + 1/p + 1/p^2 + \dots) = n/p \cdot p/(p-1) = n/(p-1),$$

   hence $v(x^n/n!) \geq nv(x) - n/(p-1) = n(v(x) - 1/(p-1))$. This shows that the series converges if $v(x) > 1/(p-1)$, hence for all $x \in p\mathbb{Z}_p$ (if p is odd) and for all $x \in 4\mathbb{Z}_2$ (otherwise). Let us show that these conditions are in fact necessary.

   If $x \in \mathbb{Z}_p^\times$, then it is clear that $v(x^n/n!) = -v(n!)$ does not tend to infinity. It remains to show that if $p = 2$ and $v(x) = 1$, then $v(x^n/n!) = n - v(n!)$ does not tend to infinity. But we have $v((2^k)!) = 2^k - 1$, so $v(x^{2^k}/(2^k)!) = 2^k - (2^k - 1) = 1$.