18. Let $P(X) \in \mathbf{Q}[X]$ be a polynomial in one variable with rational coefficients. It may happen that $P(n) \in \mathbf{Z}$ for all sufficiently large integers n without necessarily P having integer coefficients.

(a) Give an example of this.

Proof. The value of $\binom{X}{2} = \frac{1}{2}X^2 + \frac{1}{2}X$ at $X = n \in \mathbf{Z}$ is the number of ways to choose 2 elements from a collection of n, which must be integral. □

(b) Assume that P has the above property. Prove that there are integers $c_0, c_1, \ldots, c_r$ such that

$$P(X) = c_r\binom{X}{r} + c_{r-1}\binom{X}{r-1} + \cdots + c_0$$

where

$$\binom{X}{r} = \frac{1}{r!}X(X-1)\cdots(X-r+1)$$

is the binomial coefficient function. In particular, $P(n) \in \mathbf{Z}$ for all n. Thus we may call P integral valued.

Lemma. *For a sequence a_n, let Δ be the difference operator $\Delta a_n = a_{n+1} - a_n$. Then*

$$\Delta^k a_n = \sum_{i=0}^{k}\binom{k}{i}(-1)^i a_{n+k-i} \qquad \text{and} \qquad a_{n+k} = \sum_{i=0}^{k}\binom{k}{i}\Delta^i a_n.$$

Proof of lemma. By induction. Both clearly hold for $k = 0$. Suppose they hold for some k.

$$\begin{aligned}
\Delta^{k+1}a_n &= \Delta^k a_{n+1} - \Delta^k a_n \\
&= \sum_{i=0}^{k}\binom{k}{i}(-1)^i a_{n+k-i+1} + \sum_{i=0}^{k}\binom{k}{i}(-1)^{i+1}a_{n+k-i} \\
&= \binom{k}{0}a_{n+k+1} + \sum_{i=0}^{k-1}\binom{k}{i+1}(-1)^{i+1}a_{n+k-i} + \sum_{i=0}^{k-1}\binom{k}{i}(-1)^{i+1}a_{n+k-i} + \binom{k}{k}(-1)^{k+1}a_n \\
&= \binom{k+1}{0}a_{n+k+1} + \sum_{i=0}^{k-1}\binom{k+1}{i+1}(-1)^{i+1}a_{n+k-i} + \binom{k+1}{k+1}(-1)^{k+1}a_n \\
&= \binom{k+1}{0}a_{n+k+1} + \sum_{i=1}^{k}\binom{k+1}{i}(-1)^i a_{n+(k+1)-i} + \binom{k+1}{k+1}(-1)^{k+1}a_n \\
&= \sum_{i=0}^{k+1}\binom{k+1}{i}(-1)^i a_{n+(k+1)-i} \\
a_{n+k+1} &= a_{n+k} + \Delta a_{n+k} \\
&= \sum_{i=0}^{k}\binom{k}{i}\Delta^i a_n + \sum_{i=0}^{k}\binom{k}{i}\Delta^{i+1}a_n \\
&= \binom{k}{0}\Delta^0 a_n + \sum_{i=0}^{k-1}\binom{k}{i+1}\Delta^{i+1}a_n + \sum_{i=0}^{k-1}\binom{k}{i}\Delta^{i+1}a_n + \binom{k}{k}\Delta^{k+1}a_n \\
&= \binom{k+1}{0}\Delta^0 a_n + \sum_{i=0}^{k-1}\binom{k+1}{i+1}\Delta^{i+1}a_n + \binom{k+1}{k+1}\Delta^{k+1}a_n \\
&= \sum_{i=0}^{k+1}\binom{k+1}{i}\Delta^i a_n
\end{aligned}$$

□

Proof. Suppose there is some N such that $P(n) \in \mathbf{Z}$ for all $n > N$. Define a sequence $a_n = p(N + d - n + 1)$, where $d - 1$ is the degree of the polynomial. We want to show that $a_{d+1} = P(N) \in \mathbf{Z}$, since this will inductively imply that $P(n) \in \mathbf{Z}$ for all $n \in \mathbf{Z}$. For any polynomial f of degree $d-1$, the degree of $\Delta f(X)$ is strictly less than that of $f(X)$, and so $\Delta^d f(X)$ is the zero polynomial. Therefore, by the lemma, we know that $\Delta^k a_1 \in \mathbf{Z}$ for all $k \in \{1, \ldots, d\}$, since $\Delta^k a_1$ is a $\mathbf{Z}$-linear combination of $a_1, \ldots, a_{k+1}$. Since a_{d+1} is a $\mathbf{Z}$-linear combination of $a_1, \ldots, a_d$, we have $P(N) = a_{d+1} \in \mathbf{Z}$, as desired. So we have $P(\mathbf{Z}) \subseteq \mathbf{Z}$.

Now, take the sequence $a_n = P(n)$. We know the elements are integral and hence so are the kth differences. For any $n \geq d$, we have by the lemma

$$P(n) = a_n = \sum_{k=0}^{n} \binom{n}{k} \Delta^k P(0) = \sum_{k=0}^{d-1} \binom{n}{k} \Delta^k P(0)$$

because $\Delta^k P(0) = 0$ for $k \geq d$. Taking any d integers greater than d, we see that P agrees at these points with the polynomial

$$\sum_{k=0}^{d-1} \binom{X}{k} \Delta^k P(0).$$

Since d points define a degree $d-1$ polynomial, this must be $P(X)$, which thus takes the stated form. □

(c) Let $f : \mathbf{Z} \to \mathbf{Z}$ be a function. Assume that there exists an integral valued polynomial Q such that the difference function Δf defined by

$$(\Delta f)(n) = f(n) - f(n-1)$$

is equal to $Q(n)$ for all n sufficiently large positive. Show that there exists an integral-valued polynomial P such that $f(n) = P(n)$ for all n sufficiently large.

Proof. There is some N such that $\Delta f(n) = Q(n)$ for $n > N$. Define a sequence $a_n = f(N + n)$. Then $\Delta^{k+1} a_1 = \Delta^k Q(N+1)$ for all $n \in \mathbb{N}$. By the lemma, we have $P(N+k) = a_k = \sum_{i=0}^{k} \binom{k}{i} \Delta^i a_1 = a_1 + \sum_{i=0}^{k} \binom{k}{i+1} \Delta^i Q(N+1)$ for all $k \in \mathbb{N}$. Again, taking n greater than the degree $d-1$ of Q, we get

$$f(N+n) = a_1 + \sum_{i=0}^{d-1} \binom{n}{i+1} \Delta^i Q(N+1).$$

Therefore, for large n, f is the polynomial

$$f(X) = a_1 + \sum_{i=0}^{d-1} \binom{X-N}{i+1} \Delta^i Q(N+1).$$

□

1. Let $E = \mathbf{Q}(\alpha)$, where α is a root of the equation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0.$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbf{Q}$.

Proof. We employ the division algorithm:

$$(\alpha^2+\alpha+1)(\alpha^2+\alpha) = (\alpha+1)(\alpha^3+\alpha^2+\alpha+2) + (-2x-2) = -2x-2.$$

Next, we know that $\alpha - 1$ and $\alpha^3+\alpha^2+\alpha+2$ are relatively prime, we can express 1 as a linear combination of them:

$$0 = \alpha^3+\alpha^2+\alpha+2 = (\alpha^2+2\alpha+3)(\alpha-1)+5$$
$$\implies (\alpha-1)^{-1} = -\frac{1}{5}\alpha^2 - \frac{2}{5}\alpha - \frac{3}{5}.$$

□

2. Let $E = F(\alpha)$ where α is algebraic over F, of odd degree. Show that $E = F(\alpha^2)$.

   Proof. Let $2n+1$ be the degree of $F(\alpha)$. Then $\{\alpha, \alpha^2, \ldots, \alpha^{2n+1}\}$ is a basis for $F(\alpha)$ over F. $\{\alpha^2, \alpha^4, \ldots, \alpha^{2n}\}$ is linearly independent, but cannot span $F(\alpha^2)$ since the degree of this extension must divide $2n+1$. So there is some $\alpha^{2k+1} \in F(\alpha^2)$. But then $\frac{\alpha^{2k+1]}}{\alpha^{2k}} = \alpha \in F(\alpha^2)$, so $F(\alpha^2) = F(\alpha)$ (since the other inclusion is trivial). □

3. Let α and β be two elements which are algebraic over F. Let $f(X) = \min_F(\alpha)$ and $g(X) = \min_F(\beta)$. Suppose that $\deg f$ and $\deg g$ are relatively prime. Show that g is irreducible in the polynomial ring $F(\alpha)[X]$.

   Proof. Note $\deg(g) = [F(\beta) : F]$ divides $[F(\alpha,\beta) : F(\beta)]F[(\beta) : F] = [F(\alpha,\beta) : F(\alpha)]F[(\alpha) : F]$. Since $\deg(g)$ and $F[(\alpha) : F] = \deg(f)$ are relatively prime, $\deg(g)$ divides $[F(\alpha,\beta) : F(\alpha)]$, which is the degree of $\min_{F(\alpha)}(\beta)$. However, this polynomial divides g, and so $[F(\alpha,\beta) : F(\alpha)] \le \deg(g)$. Therefore, we must have the equality $\deg(g) = \deg \min_{F(\alpha)}(\beta)$, and so $g = \min_{F(\alpha)}$. Thus g is irreducible over $F(\alpha)$.

   □

4. Let α be the real positive fourth root of 2. Find all the intermediate fields in the extension $\mathbf{Q}(\alpha)$ of $\mathbf{Q}$.

   Proof. The only intermediate field is $\mathbf{Q}(\sqrt{2})$. The minimal polynomial for α is $X^4 - 2$, and $\mathbf{Q}(\alpha)$ is an extension of degree 4. An intermediate extension E must then have degree 2, and the minimal polynomial $g(X)$ of α over E must divide $X^4 - 2$. Clearly g has real coefficients, and so the only possibility is $g(X) = X^2 - \sqrt{2}$. So any intermediate extension must contain $\mathbf{Q}(\sqrt{2})$. Since this has degree 2, it *is* the only intermediate extension. □

5. If α is a complex root of $X^6 + X^3 + 1$, find all the homomorphisms $\sigma : \mathbf{Q}(\alpha) \to \mathbf{C}$.

   Proof. Because α generates the extension, its image will determine σ. Since $\sigma(\alpha)^6 + \sigma(\alpha)^3 + 1 = 0$, the only possible images for α are the roots of this polynomial. Furthermore, and such mapping gives a homomorphism, since they can be viewed as homomorphisms induced by those from $\mathbf{Q}(X)$: $\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(X^6+X^3+1)$, and such a σ contains (X^6+X^3+1) in its kernel, hence it factors through $\mathbf{Q}(\alpha)$.

   Suppose β is a root. β^3 is a root of X^2+X+1 and so is a primitive cube root of unity, thus β must be a primitive 9th root of unity. So the possible maps are $\alpha \mapsto e^{k\frac{2\pi i}{9}}$ where $k \in \{1,2,4,5,7,8\}$. □

6. Show that $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbf{Q}$, of degree 4.

   Proof. The polynomial $f(X) = X^4 - 10X^2 + 1$ has $\sqrt{2}+\sqrt{3}$ as a root. In fact, its four roots are $\pm\sqrt{3} \pm \sqrt{2}$. If f were reducible over $\mathbf{Q}$, then some product of two of these roots would have to be rational, which is obviously false. So f is the minimal polynomial of $\sqrt{2}+\sqrt{3}$, meaning this number has degree 4 over $\mathbf{Q}$. □

7. Let E, F be two finite extensions of a field k, contained in a larger field K. Show that

$$[EF : k] \leq [E : k][F : k].$$

If $[E : k]$ and $[F : k]$ are relatively prime, show that one has an equality sign in the above relation.

Proof. Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ be bases for E and F over K, respectively. Then $EF = E(\beta_1, \ldots, \beta_m)$, so $[EF : E] \leq m = [F : K]$. Therefore, the inequality holds by the tower property. Now, since $[EF : E][E : k] = [EF : F][F : k]$, if $[E : k]$ and $[F : k]$ are relatively prime then $[F : k]$ divides $[EF : E]$. Therefore, the inequality $[EF : E] \leq [F : K]$ must be an equality, and so we have $[EF : k] = [E : k][F : k]$. □