

True or false? — The answers.

Decide if the following assertions are true or not. If you think a statement is true, give an argument. If you think a statement is false, give an example demonstrating this.

(1) For any natural number n the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic.

Not true. For instance, $(\mathbb{Z}/8\mathbb{Z})^*$ is the Klein group of order 4, which is not cyclic.

(2) If R is an integral domain and $x \in R$ is an irreducible element then $(x) \subset R$ is a prime ideal.

Not true, though it is true if R is a unique factorization domain. Also, the converse (i.e., (x) prime implies x irreducible) is true. But for instance, take $R = \mathbb{C}[X, Y]/(X^2 - Y^3)$. The ring $\mathbb{C}[X, Y]$ is a unique factorization domain, and $X^2 - Y^3$ is easily seen to be an irreducible element. Hence the ideal generated by $X^2 - Y^3$ is prime, so R is a domain. Write x (resp. y) for the class of X (resp. Y) in R . Then x is irreducible but the ideal it generates is not prime, as we have $y^3 \in (x)$ but $y \notin (x)$. (Check the details yourself.)

(3) Let $f, g \in \mathbb{Q}[X]$ be irreducible polynomials of the same degree. Then the fields $\mathbb{Q}[X]/(f)$ and $\mathbb{Q}[X]/(g)$ are isomorphic.

Not true. (In fact, very far from being true!) For instance, the fields $\mathbb{Q}[X]/(X^2 - 2)$ and $\mathbb{Q}[X]/(X^2 - 3)$ are not isomorphic.

(4) Let K be a field. If $R \subset K$ is a subring with $1 \in R$ then R is an integral domain.

True, and easy to check from the definition.

(5) Let $f, g \in \mathbb{Z}[X]$ with $g \neq 0$. Then there exist $q, r \in \mathbb{Z}[X]$ with $f = q \cdot g + r$ and $r = 0$ or $\deg(r) < \deg(g)$.

Not true. It is true of course with \mathbb{Z} replaced by \mathbb{Q} . But taking $f = X$ and $g = 2X$ shows that it's not true with integral coefficients.

(6) Let R be a commutative ring. If $f, g \in R[X]$ are nonzero polynomials, $\deg(fg) = \deg(f) + \deg(g)$.

Not true. Take $R = \mathbb{Z}/4\mathbb{Z}$. Then we have $(1 + 2X) \cdot (1 - 2X) = 1$ in $R[X]$. But the assertion is true if R is a domain.

(7) Let R be a commutative ring. If $f = a_0 + a_1X + \cdots + a_nX^n$ is a unit in $R[X]$ then $f = a_0$ is a constant polynomial and $a_0 \in R^*$.

Same as for the previous question: Not true. (Same counterexample.) But true if R is a domain.

(8) Let $f \in \mathbb{Z}[X]$ be a primitive polynomial. Then f is irreducible in $\mathbb{Z}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$.

True. This is just Gauss's lemma.

- (9) Consider fields $K \subset L \subset M$. Suppose $\alpha \in M$ is algebraic over L . Further suppose that L is algebraic over K . Then α is algebraic over K .

True. Saying that α is algebraic over L means that there exists a non-zero polynomial $f = a_0 + a_1X + \cdots + a_nX^n$ in $L[X]$ with $f(\alpha) = 0$. By assumption, each of the coefficients a_i is algebraic over K . Hence the field $L' := K[a_0, \dots, a_n] \subset L$ is a finite field extension of K . Further, α is algebraic over L' , so that also $L'[\alpha]$ is a finite extension of L' . Hence $L'[\alpha]$ is a finite extension of K , so that in particular α is algebraic over K .

- (10) The fields \mathbb{R} and \mathbb{C} have the same prime field.

True. Both have \mathbb{Q} as their prime field.

- (11) A subring of a non-commutative ring is itself also non-commutative.

Not true. For instance, the ring $M_2(\mathbb{Z})$ of 2×2 matrices with integral coefficients is not commutative, but the subring of diagonal matrices is commutative.

- (12) Let $\alpha \in \mathbb{C}$. Then there exists a polynomial $f \in \mathbb{R}[X]$ with $f(\alpha) = 0$.

True. This is a special case of the general fact that every finite field extension (such as $\mathbb{R} \subset \mathbb{C}$) is algebraic.

- (13) The fields $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are isomorphic. (Here $\pi = 3, 1415\dots$ and $e = 2, 71828\dots$ are the usual constants.)

True. The numbers π and e are both transcendental over \mathbb{Q} ; hence $\mathbb{Q}[\pi]$ and $\mathbb{Q}[e]$ are both isomorphic to the ring $\mathbb{Q}[X]$ of polynomials in 1 variable over \mathbb{Q} , and their fraction fields $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are both isomorphic to the field $\mathbb{Q}(X)$ of rational functions.

- (14) Let K be a field. If $f \in K[X]$ is an irreducible polynomial of degree $d > 0$ and $K \subset L$ is decomposition field of f over K then $[L : K] = d$.

Not true. For instance, take $K = \mathbb{Q}$ and $f = X^3 - 2$. The decomposition field is the field $\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ which has degree 6 over \mathbb{Q} .

- (15) The ring $\mathbb{C}[X]$ has infinitely many prime ideals.

True. For every complex number α the ideal generated by $X - \alpha$ is prime. In fact, it is even a maximal ideal, as $(X - \alpha)$ is the kernel of the surjective homomorphism $\mathbb{C}[X] \rightarrow \mathbb{C}$ given by $f \mapsto f(\alpha)$.

- (16) If $R_1 \subset R_2$ is a subring and $I \subset R_2$ is a principal ideal then $R_1 \cap I$ is a principal ideal of R_1 .

This was perhaps the hardest of these questions. Not true. Example: Take $R_2 = \mathbb{C}[X]$, and let $R_1 = \mathbb{C}[X^2, X^3]$ be the subring of polynomials whose linear term is zero. Take

$I = (X)$. Then $R_1 \cap I$ is generated by the elements X^2 and X^3 and cannot be generated by a single element. (Once you see the example, you should have no difficulty filling in the details, so I'll leave this to you.)

- (17) Let K be a field, and let $M_n(K)$ be the ring of $n \times n$ matrices with coefficients in K . Then $M_n(K)$ has no zero divisors.

Not true, though it is of course true for $n = 1$, since $M_1(K) \cong K$. For $n = 2$ we have

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

For $n \geq 3$ the ring $M_2(K)$ is isomorphic with a subring of $M_n(K)$, so again $M_n(K)$ has zero divisors.

- (18) An infinite field has characteristic 0.

Not true. For instance, $\mathbb{F}_p[X]$ is an infinite domain of characteristic p . Its fraction field $\mathbb{F}_p(X)$ is an infinite field.

- (19) Let $\mathbb{Q} \subset K$ be a field extension of degree 6. If $\alpha \in K$ and $\alpha \notin \mathbb{Q}$ then the minimum polynomial of α over \mathbb{Q} has degree 6.

Not true. As in (14), take $K = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ and take $\alpha = \sqrt[3]{2}$ (degree 3 over \mathbb{Q}) or $\alpha = \zeta_3$ (degree 2 over \mathbb{Q}).

- (20) Same question, but now with $[K : \mathbb{Q}] = 7$.

True. In this case we have $\mathbb{Q} \subsetneq \mathbb{Q}[\alpha] \subseteq K$, and because 7 is prime we necessarily have $\mathbb{Q}[\alpha] = K$, for degree reasons.