

MATH 121 SOLUTION SET 1

1. Prove that the polynomial $p(x) = x^5 + 30x^3 + 6x + 12$ is irreducible in $\mathbb{Q}[x]$.

Solution: This polynomial is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion (with $p = 3$).

2. Let n be a positive integer. Prove that the polynomial $p(x) = 3x^n + 3x^{n-1} + \cdots + 3x^2 + 3x + 2$ is irreducible in $\mathbb{Q}[x]$.

Solution: Let us prove the following result: Suppose that F is a field, $f(x) \in F[x]$ has degree k and let $g(x) = x^k f(1/x)$. (Note that $g(x) \in F[x]$). Then if $g(x)$ is irreducible in $F[x]$ then so is $f(x)$.

To prove this, we show that if f is reducible then so is g . So suppose that $f(x) = r(x)s(x)$ for some $r(x), s(x) \in F[x]$. Then $f(1/x) = r(1/x)s(1/x)$ and hence $g(x) = x^k f(1/x) = x^k r(1/x)s(1/x)$. If we let $a = \text{degree } r(x)$ and $b = \text{degree } s(x)$ (note that $a + b = k$) then we have $g(x) = x^a r(1/x)x^b s(1/x)$. Since both $x^a r(1/x)$ and $x^b s(1/x)$ are polynomials (i.e., elements of $F[x]$) we see that $g(x)$ factors as a product of two polynomials, i.e. it is reducible.

So now we can apply this result to show that $p(x)$ is irreducible over \mathbb{Q} . Note that $x^n p(1/x) = 3 + 3x + 3x^2 + \cdots + 3x^{n-1} + 2x^n$ which is irreducible by Eisenstein's criterion (with $p = 3$). Hence we conclude that $p(x)$ is also irreducible over \mathbb{Q} .

3. Prove that the polynomial $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$ (in some extension field). Find the reciprocal of $1 + \theta$ (in the form $? + ?\theta + ?\theta^2$, where each $?$ is a rational number.)

Solution: This polynomial is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion (with $p = 3$). Alternatively, note that if it were reducible then it would have a root in \mathbb{Q} and by proposition 11 on page 308 of the text, the only possible rational roots of this polynomial are $\pm 1, \pm 2, \pm 3, \pm 6$ (these are the divisors of the constant coefficient). It is easy to check that none of these is a root of the given polynomial so it has no roots in \mathbb{Q} and hence is irreducible in $\mathbb{Q}[x]$.

To find the inverse of $(1 + \theta)$, we write down $(1 + \theta)(a + b\theta + c\theta^2) = 1$ where a, b, c are some rational numbers (to be determined). Multiplying this out and using the relation $\theta^3 + 9\theta + 6 = 0$ we get $(a - 6c) + (b + a - 9c)\theta + (c + b)\theta^2 = 1$. Since $1, \theta, \theta^2$ are linearly independent over \mathbb{Q} we get the following system of equations:

$$\begin{aligned} a - 6c &= 1 \\ b + a - 9c &= 0 \\ c + b &= 0 \end{aligned}$$

Solving this gives us $a = \frac{5}{2}, b = \frac{-1}{4}, c = \frac{1}{4}$ so that $(1 + \theta)^{-1} = \frac{5}{2} + \frac{-1}{4} \cdot \theta + \frac{1}{4} \cdot \theta^2$.

4(i). Let F be a field and $p(x) \in F[x]$ be a polynomial of degree n . Suppose a_1, \dots, a_k are distinct elements of F such that $p(a_i) = 0$ for $i = 1, \dots, k$. Prove that $k \leq n$.

Solution: Recall that if $f(x) \in F[x]$ and $a \in F$ satisfies $f(a) = 0$ then $(x - a)$ divides $f(x)$. Thus, since $p(a_1) = 0$ we see that $p(x) = (x - a_1)g_1(x)$ for some polynomial $g_1(x) \in F[x]$. Since $0 = p(a_2) = (a_2 - a_1)g_1(a_2)$ and since $a_1 \neq a_2$ we see that $g_1(a_2) = 0$ (because F is a field so it has no zero divisors) and thus $(x - a_2)$ divides g_1 . Thus we may write $p(x) = (x - a_1)(x - a_2)g_2(x)$. Then we plug in a_3 and conclude that $g_2(x)$ is divisible by $(x - a_3)$. So we continue in this manner and we see that $p(x) = (x - a_1)(x - a_2) \dots (x - a_k)h(x)$ for some $h(x) \in F[x]$. This tells us that $n = \deg p(x) = \deg(x - a_1) + \deg(x - a_2) + \dots + \deg(x - a_k) + \deg h(x)$, i.e. $n = k + \deg h(x)$. Since $\deg h(x)$ is obviously nonnegative we conclude that $k \leq n$, as was to be shown.

(ii) Suppose $f(x)$ and $g(x)$ are distinct polynomials in $F[x]$, each of degree $\leq n$. Suppose also that $f(a_i) = g(a_i)$ for $i = 1, \dots, k$, where a_1, \dots, a_k are distinct elements of F . Prove that $k \leq n$.

Solution: Define $p(x) = f(x) - g(x)$; since both f and g have degrees $\leq n$, it follows that the degree of $p(x)$ is also $\leq n$. Note that by assumption $p(a_i) = 0$ for $i = 1, \dots, k$. Then part i) of this problem tells us that $k \leq \deg p(x) \leq n$ so $k \leq n$ as was to be shown.

5. Let n be a positive integer and let $p(x) = (x - 1)(x - 2) \dots (x - n) - 1$. Prove that $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Solution: First, if $n = 1$, this polynomial is $(x - 1) - 1 = x - 2$ and it is clearly irreducible in $\mathbb{Q}[x]$ (any polynomial of degree 1 is irreducible in $\mathbb{Q}[x]$). So we may assume that $n > 1$.

Suppose $p(x)$ were reducible, say $p(x) = f(x)g(x)$. By Gauss's lemma, if $p(x)$ is reducible in $\mathbb{Q}[x]$, it is also reducible in $\mathbb{Z}[x]$ so we may assume that both $f(x)$ and $g(x)$ are elements of $\mathbb{Z}[x]$. Note that $p(1) = -1$ so that $f(1)g(1) = -1$. Thus, $f(1)$ and $g(1)$ are two integers whose product is -1 . This one of them must be equal to 1 and the other one must be equal to -1 . This means that their sum is 0. Thus, $f(1) + g(1) = 0$ or $(f + g)(1) = 0$. Similarly, $(f + g)(2) = 0, \dots, (f + g)(n) = 0$. Note that since $p(x)$ is assumed to be reducible, $\deg f(x)$ and $\deg g(x)$ are both $< n$. If $(f + g)$ were a nonzero polynomial, then on one hand we would have $\deg(f + g) \leq \max\{\deg f, \deg g\} < n$, but on the other hand part i) of the previous problem would tell us that $n \leq \deg(f + g)(x)$. This means that $(f + g)(x) = 0$ for all x so that $f(x) = -g(x)$ and thus $p(x) = f(x)g(x) = -g(x)^2$. In particular, this means that $p(x) \leq 0$ for all integers x . But $p(n + 1) = n! - 1 > 0$ (recall that

we're assuming that $n > 1$) and so this is the desired contradiction. Thus, $p(x)$ is irreducible in $\mathbb{Q}[x]$.

6. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be an automorphism of the field \mathbb{R} . (That is, suppose $f : \mathbb{R} \rightarrow \mathbb{R}$ is a bijection such that $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{R}$.) Prove that f is the identity map.

Solution: First, note that for any real number x we have $f(x^2) = (f(x))^2$. Thus, f maps squares to squares. Since any positive real number is a square (i.e. if $x \in \mathbb{R}, x > 0$ then there exists $y \in \mathbb{R}$ such that $x = y^2$; simply take $y = \sqrt{x}$), it follows that f maps positive real numbers to positive real numbers. From this we conclude that f preserves inequalities: if $a < b$ then $f(a) < f(b)$. (To see this, note that $a < b$ is the same as $b - a > 0$. Since f maps positive numbers to positive numbers, we have $f(b - a) > 0$ which implies that $f(b) > f(a)$).

Next, I claim that the restriction of f to \mathbb{Q} is the identity map. (This just means that $f(q) = q$ for all $q \in \mathbb{Q}$.) To see this, note first that $f(1) = f(1^2) = (f(1))^2$ so that $f(1) = 0$ or 1 but since f is injective and $f(0) = 0$ we must have $f(1) = 1$. Next, for any real number x and any nonnegative integer m we have $f(mx) = f(x + x + \cdots + x) = f(x) + f(x) + \cdots + f(x) = mf(x)$ (one could prove this formally using mathematical induction). Also, if $m < 0$ then $-m > 0$ and then we have $0 = f(0) = f(mx + (-mx)) = f(mx) + f(-mx) = f(mx) + (-m)f(x)$ and so $f(mx) = -(-m)f(x) = mf(x)$. Since $f(0) = 0$ we have $f(mx) = mf(x)$ for all integers m . Next, $1 = f(1) = f(m \cdot \frac{1}{m}) = m \cdot f(1/m)$ so that $f(1/m) = 1/m$ for all nonzero integers m . Finally, $f(m/n) = f(m \cdot \frac{1}{n}) = mf(1/n) = m/n$. Since any rational number is of the form m/n for some integers m, n it follows that the restriction of f to \mathbb{Q} is the identity map.

Next, we'll show that f must be continuous. First, note that if m is an integer such that $\frac{-1}{m} < b - a < \frac{1}{m}$ then (since f preserves inequalities, as we saw above) we have $\frac{-1}{m} < f(b) - f(a) < \frac{1}{m}$. Next, let $a \in \mathbb{R}$, $\epsilon > 0$, let $\delta = \epsilon$ and let m be an integer such that $0 < |x - a| < \frac{1}{m} < \epsilon$. Then, as we just saw, this implies that $0 < |f(x) - f(a)| < \frac{1}{m} < \epsilon$ and thus f is continuous at a . Since a was arbitrary, we conclude that f is indeed continuous on \mathbb{R} .

Finally, recall the following fact from Real Analysis: If two continuous functions agree on a dense set then they agree everywhere on their domain. Since \mathbb{Q} is dense in \mathbb{R} and both f and the identity functions are continuous on \mathbb{R} and they agree on \mathbb{Q} , it follows that they must agree everywhere, i.e. f must be the identity function. (If you have not seen the concept of a dense set or if you have not seen the fact from Real Analysis I just mentioned, the proof can be completed as follows. We must show that $f(x) = x$ for all $x \in \mathbb{R}$. We have already seen that this is true if $x \in \mathbb{Q}$. If x is irrational, choose a sequence of rational numbers x_n such that x_n converges to x . By continuity of f , $f(x_n)$ converges to $f(x)$. But each x_n is rational, so $f(x_n) = x_n$ and so x_n converges to $f(x)$. Since x_n also converges to x we conclude that $f(x) = x$. Since x was an arbitrary irrational number we conclude that $f(x) = x$ for all $x \in \mathbb{R}$ as was to be shown.)

7. Let E be a finite extension field of \mathbb{Q} . (In other words, let E be a field containing \mathbb{Q} as a subfield such that $[E : \mathbb{Q}]$ is finite.) Prove that E is not isomorphic to any proper subfield of E .

Solution: Let K be a subfield of E such that K is isomorphic to E . We'll show that in fact $K = E$. Let $f : K \rightarrow E$ be a (field) isomorphism. Note that both K and E can be viewed as vector spaces over \mathbb{Q} . Note that f is also a vector space isomorphism; indeed, we know that f is a bijection and preserves addition because f is a field isomorphism. Also, for any rational number q we have $f(qe) = f(q)f(e) = qf(e) = qf(e)$ (the proof that $f(q) = q$ is essentially the same as the one we gave in the previous problem). So f may be viewed as a linear transformation from K to E and thus it is a vector space isomorphism. From linear algebra we know that two finite dimensional vector spaces are isomorphic if and only if they have the same dimension; hence we have $[E : \mathbb{Q}] = [K : \mathbb{Q}]$. But since K is a subfield of E we have $[E : \mathbb{Q}] = [E : K][K : \mathbb{Q}] = [E : K][E : \mathbb{Q}]$ and since $[E : \mathbb{Q}] < \infty$ we conclude that $[E : K] = 1$ so $E = K$ as was to be shown.