

421 HW 5 Group

change this to your names

Note: R denotes a ring and F denotes a field and p denotes a positive prime number.

Problem (4.1.17). Let R be an integral domain. Assume that the Division Algorithm always holds in $R[x]$. Prove that R is a field.

Solution. Statement of the division algorithm: given $f \in F[x]$ and $g \in F[x]$, there exist some polynomials p and r such that $f = gp + r$ and either $r = 0$ or degree of r is less than degree of g .

Suppose that a is an arbitrary nonzero element of R .

By the Division Algorithm, there exists some p and r for which $1 = pa + r$, where r is either 0 or has degree less than a . a has degree 0, so it must be that $r = 0$. Thus, $1 = pa$. a has an inverse.

Since a was an arbitrary nonzero element of R , every nonzero element of R has a multiplicative inverse. Therefore, R is a field.

Problem (4.2.14). Let $f(x), g(x), h(x) \in F[x]$, with $f(x)$ and $g(x)$ relatively prime. If $f(x) \mid h(x)$ and $g(x) \mid h(x)$, prove that $f(x)g(x) \mid h(x)$.

Solution.

Problem (4.3.12). Express $x^4 - 4$ as a product of irreducibles in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and in $\mathbb{C}[x]$.

Solution.

$$\begin{array}{ll} \mathbb{Q}[x] & (x^2 + 2)(x^2 - 2) \\ \mathbb{R}[x] & (x^2 + 2)(x - \sqrt{2})(x + \sqrt{2}) \\ \mathbb{C}[x] & (x - i\sqrt{2})(x + i\sqrt{2})(x - \sqrt{2})(x + \sqrt{2}) \end{array}$$

Problem (4.4.16). Let $f(x), g(x) \in F[x]$ have degree $\leq n$ and let c_0, c_1, \dots, c_n be distinct elements of F . If $f(c_i) = g(c_i)$ for $i = 0, 1, \dots, n$, prove that $f(x) = g(x)$ in $F[x]$.

Solution. For $i \in 0, 1, \dots, n$, it is said that $f(c_i) = g(c_i)$. With subtraction, $f(c_i) - g(c_i) = 0$. Since the degree of f and degree of g are both $\leq n$, it must be that $f - g = 0$ or the degree of $f - g$ is $\leq n$.

If $f - g$ is nonzero, since the degree of $f - g$ is $\leq n$, then $f - g$ must have at most n roots. This is not the case, as it is said to have $n + 1$ roots.

$f - g$ must therefore be the zero polynomial.

$f(x) - g(x) = 0$, so $f(x) = g(x)$.

Problem (4.4.19). We say that $a \in F$ is a multiple root of $f(x) \in F[x]$ if $(x - a)^k$ is a factor of $f(x)$ for some $k \geq 2$.

(a) Prove that $a \in \mathbb{R}$ is a multiple root of $f(x) \in \mathbb{R}[x]$ if and only if a is a root of both $f(x)$ and $f'(x)$, where $f'(x)$ is the derivative of $f(x)$.

(b) If $f(x) \in \mathbb{R}[x]$ and if $f(x)$ is relatively prime to $f'(x)$, prove that $f(x)$ has no multiple root in \mathbb{R} .

Solution. (a)

Suppose $x - a$ is a multiple root of polynomial $f(x) \in \mathbb{R}[x]$. This means that $(x - a)^k$ is a factor of f , for some $k \geq 2$. Let f be rewritten as $g(x - a)^k$, where $x - a$ does not divide g .

By the product rule of differentiation,

$$\begin{aligned} f &= g(x - a)^k \\ f' &= g'(x - a)^k + gk(x - a)^{k-1} \\ f' &= (x - a)^{k-1}(g'(x - a)^k + gk) \end{aligned}$$

If $k \geq 2$, then $k - 1 \geq 1$, so $x - a$ is a factor of f' .

This proves the forward direction.

For the backward direction,

Suppose that $f' = (x - a)g$ and $f = (x - a)h$ for some polynomials g and h .

Through differentiation, $f' = (x - a)h' + h$.

$$\begin{aligned} f' &= (x - a)g \\ f' &= (x - a)h' + h \\ (x - a)g &= (x - a)h' + h \\ (x - a)(g - h') &= h \end{aligned}$$

Substituting into an earlier equation, $f = (x - a)(x - a)(g - h')$.

$(x - a)^k$ is a factor of f for some $k \geq 2$. Therefore, $x - a$ is a multiple root.

The theorem is proven.

(b)

The forward statement above is the following, under the conditions that $k \geq 2$ and $f(x) \in \mathbb{R}[x]$:

$$(x - a)^k \mid f \implies (x - a) \mid f \text{ and } (x - a) \mid f'$$

Its contrapositive is

$$(x - a) \nmid f \text{ or } (x - a) \nmid f' \implies (x - a)^k \nmid f$$

Suppose that, for every $a \in \mathbb{R}$, $x - a \nmid f$ and $x - a \nmid f'$.

This means that, for any $k \geq 2$, $(x - a)^k \nmid f$.

The theorem is proven.