Mathematics 310
Robert Gross
Homework 8
Answers

In all of these problems, F is a field.

1. Let $f = x^3 + 1$ and $g = 2x^4 + 3$ be polynomials in $\mathbf{F}_7$. Let $d = (f, g)$. Use the Euclidean algorithm to find d and to find polynomials a and b so that $af + bg = d$. *Note*: Remember that d is monic.

Answer: We start by dividing x^3+1 into $2x^4+3$. We see that the quotient is $2x$, and $2x^4+3 = (2x)(x^3+1)+(5x+3)$. Now, divide $5x+3$ into x^3+1, and we get $x^3+1 = (5x+3)(3x^2+x+5)$. Therefore, a greatest common divisor is $5x+3$, and we have $5x+3 = (1)(2x^4+3)+(5x)(x^3+1)$. However, we require that the greatest common divisor be monic, so we must multiply this equation by 3, yielding $x + 2 = (3)(2x^4 + 3) + (x)(x^3 + 1)$.

2. Suppose that $f, g, h \in F[x]$,with $(f, g) = 1$, $f|h$, and $g|h$. Prove that $fg|h$.

Answer: Write $1 = af + bg$. Multiply by h, and we have $h = afh + bgh$. Now, $g|h$ and so $fg|afh$. Similarly, $f|h$, so $fg|bgh$. Therefore, $fg|h$.

3. Let $I = (f)$ and $J = (g)$ be ideals in $F[x]$. Show that $I \subset J$ if and only if $g|f$.

Answer: (a) Suppose first that $g|f$. Write $f = qg$. Take any element $h \in I$. We know that $h = pf$ because $I = (f)$. Then $h = pqg$, so $h \in (g) = J$. Therefore $I \subset J$.

(b) Suppose instead that $I \subset J$. Because $f \in I$, we know that $f \in J$, and therefore $f = qg$. Therefore, $g|f$.

4. Suppose that K and L are fields, with $K \subset L$ and $f, g \in K[x]$. Suppose that f and g are relatively prime as elements of $K[x]$. Prove that f and g remain relatively prime when considered as elements of $L[x]$.

Answer: Because f and g are relatively prime, we can find polynomials $a, b \in K[x]$ so that $af + bg = 1$. Now, suppose that $d \in L[x]$ divides by f and g. The equation $af + bg = 1$ shows that $d|1$, and therefore $d \in L$. This shows that f and g are still relatively prime when considered as elements of $L[x]$.

5. Suppose that I and J are ideals in a commutative ring R. Define $I + J = \{i + j : i \in I, j \in J\}$.

(a) Show that $I + J$ is an ideal of R.

(b) Show that $I \cap J$ is an ideal of R.

Answer: (a) Take $i_1+j_1, i_2+j_2 \in I+J$. Then $(i_1+j_1)+(i_2+j_2) = (i_1+i_2)+(j_1+j_2) \in I+J$, so $I+J$ is closed under multiplication. Now take $r \in R$, and then $r(i_1+j_1) = ri_1+rj_1 \in I+J$, so $I + J$ has the correct multiplicative property, making $I + J$ an ideal.

(b) Take $r_1, r_2 \in I \cap J$. Then $r_1, r_2 \in I$, so $r_1 + r_2 \in I$, and similarly $r_1 + r_2 \in J$, so $r_1 + r_2 \in I \cap J$. Take $r \in r$, and then $rr_1 \in I$ because I is an ideal, and similarly $rr_1 \in J$ because J is an ideal. Therefore $rr_1 \in I \cap J$, making $I \cap J$ an ideal.

6. Suppose that I and J are ideals of $\mathbf{Z}$, with $I = (m)$ and $J = (n)$.

(a) Let $r = [m, n]$, the least common multiple of m and n. Show that $I \cap J = (r)$.

(b) Let $d = (m, n)$. Show that $I + J = (d)$.

Answer: (a) We know that we can write $I \cap J = (t)$, where t is the smallest positive element in $I \cap J$. We know that $I \cap J \subset I$, and so a problem above tells us that $m|t$. Similarly, we know that $I \cap J \subset J$, so $n|t$. Therefore, $[m, n]|t$. However, it is also clear that $[m, n] \in I \cap J$, so $I \cap J = ([m, n])$.

(b) We know that we can find integers x and y so that $mx + ny = d$. Because $mx \in I$ and $ny \in J$, we know that $d \in I + J$.

On the other hand, take any element $p \in I + J$, and we know that we can write $p = mr + ns$. Because $d|m$ and $d|n$, we know that $d|p$. Therefore $I + J = (d)$.