Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 23, 2020

Problems in Section 3.9.

1. Find the greatest common divisor of the following polynomials over F, the field of rational numbers.
a) $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$.

Solution. Observe that

$$
\begin{aligned}
x^5 - 6x + 1 &= (x^2 + 6x + 35)(x^3 - 6x^2 + x + 4) + 200x^2 - 65x - 139, \\
x^3 - 6x^2 + x + 4 &= \left(\frac{x}{200} - \frac{227}{8000}\right)(200x^2 - 65x - 139) + \left(-\frac{239}{1600}x + \frac{447}{8000}\right), \\
200x^2 - 65x - 139 &= \left(-\frac{320000}{239}x - \frac{3752000}{57121}\right)\left(-\frac{239}{1600}x + \frac{447}{8000}\right) - \frac{7730176}{57121}, \\
-\frac{239}{1600}x + \frac{447}{8000} &= \left(\frac{13651919}{12368281600}x - \frac{25533087}{61841408000}\right)\left(-\frac{7730176}{57121}\right) + 0
\end{aligned}
$$

Thus the greatest common divisor of $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$ is 1. □

b) $x^2 + 1$ and $x^6 + x^3 + x + 1$.

Solution. Note that $x^6 + x^3 + x + 1 = (x^4 - x^2 + x + 1)(x^2 + 1)$ so that their greatest common divisor is $x^2 + 1$. □

2. Prove that
a) $x^2 + x + 1$ is irreducible over F, the field of integers mod 2.

Proof. Substituting $x = 0$ and $x = 1$ both to $x^2 + x + 1$ yields 1 mod 2, so that $x^2 + x + 1$ is irreducible over F. □

b) $x^2 + 1$ is irreducible over the integers mod 7.

Proof. Note that for prime p, $x^2 + 1 \equiv 0 \pmod{p}$ has solution only if p is a prime of form $4k + 1$. But $7 = 4 \cdot 1 + 3$, so that $x^2 + 1 \not\equiv 0 \pmod{7}$. Hence, $x^2 + 1$ is irreducible over F. $\square$

c) $x^3 - 9$ is irreducible over the integers mod 31.

Proof. Note that given polynomial is degree of 3. So if it was reducible, it must have at least one polynomial of degree 1 as its factor. Hence, it admits a root. Thus, assume that $x^3 \equiv 9 \pmod{31}$ for some x. By FLT, $x^{30} \equiv 1 \pmod{31}$. Consequently,

$$x^{30} \equiv 9^{10} \equiv 5 \not\equiv 1 \pmod{31},$$

which is a contradiction. Hence, $x^3 - 9$ is irreducible over F. $\square$

d) $x^3 - 9$ is reducible over the integers mod 11.

Proof. $x = 4$ gives $4^3 = 64 \equiv 9 \pmod{11}$. Hence, $(x - 4)$ is a factor of $x^3 - 9$ in F. Thus, $x^3 - 9$ is reducible over F. $\square$

3. Let F, K be two fields $F \subset K$ and suppose $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$. Prove that they are relatively prime in $K[x]$.

Proof. As $f(x), g(x)$ are relatively prime in $F[x]$, there exists $\lambda(x), \mu(x) \in F(x)$ and an unit $k \in F[x]$ such that

$$f(x)\lambda(x) + g(x)\mu(x) = k.$$

Now merely consider the above equation as an equation in $K[x]$. Since units in $F[x]$ is also units in $K[x]$, $f(x)$ and $g(x)$ are relatively prime in $K[x]$ too. $\square$

4. a) Prove that $x^2 + 1$ is irreducible over the field F of integers mod 11 and prove directly that $F[x]/(x^2 + 1)$ is a field having 121 elements.

Proof. Note that for a prime p, equation $x^2 + 1$ mod p admits a root only if p is a prime of form $4k + 1$. But $11 = 4 \cdot 2 + 3$, so that $x^2 + 1$ has no root in F. Thus, $x^2 + 1$ is irreducible in F. Consequently, $((x^2 + 1))$ is a maximal ideal in $F[x]$ so that $F[x]/(x^2 + 1)$ is a field. Since every element in this field is expressible in a way that;

$$\frac{F[x]}{(x^2 + 1)} = \left\{ ax + b + (x^2 + 1) \mid a, b \in F \right\},$$

hence there are $11 \cdot 11 = 121$ distinct elements in this field. $\square$

b) Prove that $x^2 + x + 4$ is irreducible over F, the field of integers mod 11 and prove directly that $F[x]/(x^2 + x + 4)$ is a field having 121 elements.

Proof. Since $f(x) = x^2 + x + 4$ is a polynomial of degree 2, we check if it admits a root or not. By simple calculations, $f(0) \equiv f(10) \equiv 4 \pmod{11}$, $f(1) \equiv f(9) \equiv 6 \pmod{11}$, $f(2) \equiv f(8) \equiv -1 \pmod{11}$, $f(3) \equiv f(7) \equiv 5 \pmod{11}$, $f(4) \equiv f(6) \equiv 2 \pmod{11}$, $f(5) \equiv 1 \pmod{11}$. Hence, $f(x)$ is irreducible in F. And similarly as in Problem 4, $F[x]/(f(x))$ is a field with 121 elements. □

c) Prove that the fields of part a) and part b) are isomorphic.

Proof. We build a homomphism between $F[x]/(x^2+1)$ and $F[x]/(x^2+x+4)$. Suppose $\phi : F[x]/(x^2+1) \to F[x]/(x^2+x+4)$. Suppose $\phi(x) = a + bx$. Then

$$\phi(x^2+1) = \phi(x)^2 + \phi(1) = (a+bx)^2 + a = b^2x^2 + 2abx + (a^2+a)$$

must divide $x^2 + x + 4$ so that $b^2x^2 + 2abx + (a^2+a) = b^2x^2 + b^2x + 4b^2$. On solving this,

$$2ab = b^2, \quad a^2 + a = 4b^2 \pmod{11} \implies a = 3,\ b = 6.$$

Thus, $\phi(x) = 3 + 6x$. We know this yields a bijection. To check this is a homomorphism, $\phi((a+bx)+(c+dx)) = \phi((a+c)+(b+d)x) = 3(a+c)+6(b+d)x = \phi(a+bx)+\phi(c+dx)$. Also, we can check that $\phi((a+bx)(c+dx)) = \phi(a+bx)\phi(c+dx)$ similarly. Therefore, $F[x]/(x^2+1)$ and $F[x]/(x^2+x+4)$ are isomorphic. □

5. Let F be the field of real numbers. Prove that $F[x]/(x^2+1)$ is a field isomorphic to the field of complex numbers.

Proof. Note that x^2+1 is irreducible in $\mathbb{R} = F$. Thus, $F[x]/(x^2+1)$ is a field, with elements of the form $a + bx + (x^2+1)$, $a, b \in F$. We now define a mapping $\phi : F[x]/(x^2+1) \to \mathbb{C}$ by $\phi(a+bx+(x^2+1)) = a+bi$. Is it well defined? Suppose $a+bx+(x^2+1) = c+dx+(x^2+1)$. Then $a-c+(b-d)x \in (x^2+1)$ so that $(a-c)+(b-d)x = 0, a = c, b = d$. Thus, $a+bi = c+di$ and hence ϕ is well defined. We check if ϕ is a homomorphism. Observe that

$$\begin{aligned}
\phi((a+bx+(x^2+1))+(c+dx+(x^2+1))) &= \phi((a+c)+(b+d)x+(x^2+1)) \\
&= (a+c)+(b+d)i = (a+bi)+(c+di) \\
&= \phi(a+bx)+\phi(c+dx), \\
\phi((a+bx)(c+dx)+(x^2+1)) &= \phi((ac-bd)x+(ad+bc)x+(x^2+1)) \\
&= (ac-bd)+(ad+bc)i = (a+bi)(c+di) \\
&= \phi(a+bx+(x^2+1))\phi(c+dx+(x^2+1)).
\end{aligned}$$

Thus, ϕ is a homomorphism. Also, it is clearly surjective. Now we consider its kernel. Suppose $\phi(a+bi+(x^2+1)) = a+bi = 0$. Then $a = 0, b = 0$ so that $\phi(a+bi+(x^2+1)) = 0 \iff \phi((x^2+1)) = 0$. Hence, ϕ is injective. Therefore, we have established an onto isomorphism between $F[x]/(x^2+1)$ and $\mathbb{C}$. □

6. Define the derivative $f'(x)$ of the polynomial

$$f(x) = a + 0 + a_1 x \cdots + a_n x^n$$
$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

Prove that if $f(x) \in F[x]$, where F is the field of rational numbers, then $f(x)$ is divisible by the square of a polynomial if and only if $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree.

Proof. Suppose $f(x)$ is divisible by $q(x)^2$, where $deg(q(x)) \geq 1$. Then $f(x) = k(x)q(x)^2$ for some $k(x) \in F[x]$. Consequently, $f'(x) = k'(x)q(x)^2 + 2k(x)q(x)q'(x)$ so that $q(x) \mid f'(x)$. Let $d(x)$ be the greatest common divisor of $f(x)$ and $f'(x)$. Since $deg(d(x)) \geq deg(q(x)) \geq 1$, We are done. Conversely, assume that $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree. Then there exists a prime(irreducible) polynomial $p(x)$ which divides both $f(x)$ and $f'(x)$. Let $f(x) = t(x)p(x)$. Then $f'(x) = t'(x)p(x) + t(x)p'(x)$, so that $p(x) \mid p'(x)t(x)$. As $deg(p(x)) > deg(p'(x))$, $p(x) \nmid p'(x)$ and since $p(x)$ is prime, $p(x) \mid t(x)$. That is, $t(x) = s(x)p(x)$ for some $s(x) \in F[x]$ Thus, $f(x) = s(x)p(x)^2$ and hence $p(x)^2 \mid f(x)$. □

7. If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ is irreducible over F of degree n prove that $F[x]/(f(x))$ is a field with p^n elements.

Proof. Note that $F[x]/(f(x))$ is clearly a field since $f(x)$ is irreducible over $F[x]$. Now since $F[x]$ being an Euclidean ring, division algorithm in $F[x]$ assures the uniqueness of the remainder of any polynomial on division by $f(x)$. Hence, any elements in $F[x]/(f(x))$ must be a polynomial of degree less than $n = deg(f(x))$ and vice versa, it consists of p^n elements in total. □