Solution of Algebra III Mid-sem 2009

August 24, 2016

Question 1: Find all automorphisms of $\mathbb{Z}[X]$. Conclude that given a fixed integer c, every element of $\mathbb{Z}[X]$ can be written uniquely as a polynomial in $X - c$ with integer coefficients.

Solution: Since X is the generator of $\mathbb{Z}[X]$, for any automorphism f of $\mathbb{Z}[X]$, $f(X)$ will also be a generator. Therefore $f(X)$ must be a linear polynomial of the form $aX + b$, a, b are integers. Since f is surjective we have

$$X = cf(X) + d = acX + bc + d$$

so we have $ac = 1$, hence $a = 1$ or -1. Therefore $f(X) = X + b$ or $-X + b = -(X - b)$. From this we conclude that any polynomial can be written uniquely as a polynomial in $X - c$, for any integer c.

Question 2: Let I, J be ideals in R such that $I + J = R$.

Prove that : a) $I \cap J = IJ$. b) R/IJ is isomorphic to $R/I \times R/J$. Find the idempotents of R/IJ corresponding to this decomposition.

Solution: By definition IJ is contained in $I \cap J$. Let a belong to $I \cap J$. Since $I + J = R$, there exists b, c in I, J respectively such that $b + c = 1$. Then we have $a = ab + ac$, which is in IJ. So we get that $I \cap J = IJ$.

Define the homomorphism ϕ from R/IJ to $R/I \times R/J$, by the following rule

$$\phi(a + IJ) = (a + I, a + J)\ .$$

It is easy to check that it is a well defined homomorphism. Suppose that $\phi(a + IJ) = 0$, that means that a belongs to $I \cap J$. Since $I \cap J = IJ$, we have a belongs to IJ. So ϕ is injective. Now we have to prove that ϕ is surjective. So let us take $(b + I, c + J)$ in $R/I \times R/J$. We need to produce $a \in R$ such that $a + I = b + I, a + J = c + J$. That is we need a such that $a - b$ belongs to I and $a - c$ belongs to J. Consider x, y in R such that $x + y = 1$. Then $\phi(x + IJ) = (0, 1 + J)$ and $\phi(y + IJ) = (1 + I, 0)$. Then

$$\phi(cx + by + IJ) = (cx + by + I, cx + by + J) = (c + I, c + J)(0, 1 + J) + (b + I, b + J)(1 + I, 0)$$

that is equal to

$$(b + I, c + J)\ .$$

So ϕ is an isomorphism.

Idempotents of R/IJ corresponds to idempotents in $R/I \times R/J$ by this isomorphism.

Question 3: a) Show that an ideal P is a prime ideal in R if and only if R/P is an integral domain.

b) Let $f : R \to D$ be a ring homomorphism into an integral domain D. Given two ideals in D, let I, J be their inverse images under f. Suppose that the product IJ is contained in $ker(f)$. Then prove that I or J is equal to $ker(f)$. Is it necessary that IJ equals to $ker(f)$.

Solution

a) Let P be a prime ideal. To prove that R/P is an integral domain. So let $a + P.b + P = 0 = ab + P$, that means ab belongs to P, since P is prime we have that $a \in P$ or $b \in P$. So $a + P = 0$ or $b + P = 0$.

Suppose that R/P is an integral domain. Let ab belongs to P. Then we have $ab+P = (a+P)(b+P) = 0$, which shows that $a \in P$ or $b \in P$. So P is prime.

b) Since D is an integral domain, we observe that $ker(f)$ is a prime ideal. Suppose that IJ is contained in $ker(f)$. Suppose also that I and J both are not contained in $ker(f)$. So there exists a, b in I, J which are not in $ker(f)$ such that ab belongs to $ker(f)$. This contradicts that $ker(f)$ is prime. So either I or J is contained in $ker(f)$. On the other hand $ker(f)$ is contained in I, J (Since $\{0\}$ is contained in their images under f). If $IJ = Ker(f) = I$, then I is contained in $I \cap J$, meaning that $I \subset J$, which may not be true.

Question 4: For an element R in the ring R, consider the ideal $(rX - 1)$ in $R[X]$. Consider the natural homomorphism $\Phi : R \to S = R[X]/I$.

a)Show that $ker(\Phi)$ is
$$\{a : r^n a = 0, n \in \mathbb{N}\} .$$

b)Conclude that $S = 0$ if and only if r is nilpotent in R.

c)Show that Φ is an isomorphism if and only if r is a unit in R.

Solution:a) First we prove that the ring $S = R[X]/I$, is the ring R_r, that is R localized at r. So define a homomorphism $\Psi : S \to R_r$, given by
$$f \mapsto f(1/r) .$$
Since in the ring S we have $x = 1/r$, the map well defined homomorphism. It is easily seen to be a surjection. We have to prove that Ψ is an injection. So suppose that $f(1/r) = 0$, that means that
$$a_0 + a_1(1/r) + \cdots + a_n(1/r)^n = 0$$
which gives us that
$$r^n a_0 + r^{n-1}a_1 + \cdots + a_n/r^n = 0$$
that is by definition we have
$$r^s(r^n a_0 + r^{n-1}a_1 + \cdots + a_n) = 0$$
which gives us that $a_i = 0$ for all i. Therefore it will follow that $\Phi(a) = 0$, means that $a/1 = 0$ in the localization R_r. Which by definition is equivalent to $r^n a = 0$, for some $n \in \mathbb{N}$.

b) We have to prove that $S = 0$ if r is a nilpotent in R. Suppose that r is a nilpotent. That is $r^n = 0$ for some n. Then any a/r^m can be written as $r^n a/r^{m+n}$. But $r^n = 0$, so we have $a/r^m = 0$.

On the other hand suppose that $S = 0$. Then $1/r^n = 0$ in S, which means that there exists m such that $r^m = 0$. So r is a nilpotent.

c) The map Φ is an isomorphism means that $a/ \mapsto a/1$ is an isomorphism. Suppose that r is a unit. Suppose that $a/1 = 0$, meaning that there exists m such that $r^m a = 0$. Since r is a unit we have that r^m a unit hence $a = 0$. So the map is an injection. Let us consider an element a/r^n, then it there is ar^{-n} which maps to this element. Hence the map is surjective, hence an isomorphism.

Suppose that Φ is an isomorphism. We have to prove that r is a unit. Let $a/1 = 1/r$, which gives us that there exists n such that
$$r^n(ra - 1) = 0$$

this implies that $ra - 1 = 0$ (because it is in the kernel of Φ), so we have that $ra = 1$.

Question 5: Let M be a proper ideal in R.

a) Show that the statement "All elements in $R - M$ are units" is equivalent to the statement "M is the unique maximal ideal in R".

b) Using the knowledge about units in the power series ring $\mathbb{Q}[[X]]$, state why the equivalent conditions holds for this ring.

c) Show that there is a unique homomorphism $\mathbb{Q}[[X]] \to \mathbb{Q}$. Is this statement holds for an arbitrary field F.

<u>Solution</u>: a) Let M be the unique maximal ideal in R. Let a belong to $R - M$. Then the ideal generated by a must be contained in a maximal ideal if it is not a unit. But there is only maximal ideal M which does not contain a. So the ideal generated by a is R. Hence a a unit.

On the other hand suppose that there exists M_1 a maximal ideal which is not equal to M. Then there exists a in $M_1 - M$. Since all elements of $R - M$ is a unit, a must be a unit. So we have that $M_1 = R$. Hence M is unique.

b)the ideal generated by x is the unique maximal ideal because any power series which has a non-zero constant term is a unit. So the above conditions hold in the case of $\mathbb{Q}[[X]]$.

c) Any homomorphism f from $\mathbb{Q}[[X]]$ to $\mathbb{Q}$ is identity on $\mathbb{Q}$. So it is surjective. The inverse image of the zero ideal in $\mathbb{Q}$, under f is maximal (this is because inverse image of a maximal ideal under a surjective homomorphism is a maximal ideal). Since the ideal generated by X is the only maximal ideal in $\mathbb{Q}[[X]]$, we have that $ker(f)$ is equal to the ideal generated by X. So we have that the homomorphism f is unique and determined by the ideal $< X >$. Here we used the divisibility property of $\mathbb{Q}$, that is for any integer n we have that $n.1/n = 1$, which may not hold for arbitrary field F.

Question: a) Let R be a PID and S a UFD, with R contained in S. Let d be the gcd of a, b in R, where a, b are non-zero non-units. Show that d is also the gcd of a, b in S.

b) Find a gcd of $11 + 7i$ and $18 - i$ in the ring of Gaussian integers $\mathbb{Z}[i]$.

<u>Solution</u>: Since S is a UFD, we have that the factorization of a, b remain unique in R, S. Therefore the gcd remain unique.

We describe the general procedure for finding the GCD of two Gaussian integers. Let us have $\alpha = a + ib, \beta = c + id$ two numbers. Then consider $a + ib/c + id = \alpha/\beta = r + is$, where $r = ac + bd/c^2 + d^2, s = ad - bc/c^2 + d^2$. Find p, q integers in $\mathbb{Z}$ such that $|r - p|, |q - p|$ are less than or equal to $1/2$. Put $\theta = (r - p) + i(s - q)$ and set $\gamma = \beta\theta$, then we get that

$$\alpha = \beta(p + iq) + \gamma$$

since $N(\theta)$ is less than or equal to $1/2$ we have that $N(\gamma)$ is less or equal to $N(\beta)/2$. Continue this process until $N(\gamma) = 0$.

Question: Given two polynomials f, g in $\mathbb{C}[X, Y]$ let $I = (f, g)$, the ideal generated by f, g. Prove that $\mathbb{C}[X, Y]/I$ is a finite dimensional vector space if and only if the GCD $(f, g) = 1$.

<u>Solution</u> First we prove that if the variety defined by $f = g = 0$ has finitely many points then GCD of f, g is 1 and vice versa.

Suppose that the gcd is 1. Then the varieties defined by zero locus of f, g must intersect at finitely many points. Otherwise gcd will not be 1.

Now suppose that we have $f = 0$ intersect $g = 0$ at finitely many points. Then let gcd be d which is a polynomial of degree greater or equal than 1. Then we have $d = 0$ is contained in the intersection $f = g = 0$, which is impossible since $d = 0$ defines a curve.

Now we prove that the variety $f = g = 0$ has finitely many points is equivalent to the fact that dimension of $\mathbb{C}[X, Y]/I$ is finite.

Suppose that $f = g = 0$ has finitely many points $P_1, \cdots, P_n$. Then by Chinese remainder theorem we have that

$$\mathbb{C}[X, Y]/I \cong \prod_i \mathbb{C}[X, Y]/I(P_i)$$

the right hand side is finite dimensional so we have $\mathbb{C}[X, Y]/I$ is finite dimensional.

Suppose that $\mathbb{C}[X, Y]/I$ is of finite dimension. Then it is Artinian as a ring hence has Krull dimension zero, so we get that $f = g = 0$ consists of finitely many points.

Question 8: Let R be a commutative ring. Describe the kernel of the map $\phi : R[X, Y] \to R[T]$ such that ϕ is identity on R, $\phi(X) = T^p, \phi(Y) = T^q$. p, q are relative prime positive integers.

Solution Suppose that $\phi(f) = 0$, that is $f(X, Y) = \sum_{i,j} a_{ij} X^i Y^j$ is mapped to zero under ϕ. That is

$$\sum_{i,j} a_{ij} T^{pi+qj} = 0\ .$$

Already we have $X^q - Y^p$ is in the kernel. We prove that it generates the kernel. So let f belong to the kernel, then we have

$$\phi(f) = 0 = \sum_i a_i T^{pi} + \sum b_j T^{qj} + \sum_{kl} c_{kl} X^k Y^l$$

the above implies that $c_{kl} = 0$ and $a_i = b_j = 0$ except for $pi = qj = m$ and in this case we have $a_i = -b_j$. Then we have that f is a linear combination of polynomials of the form $X^{qk} - Y^{pk}$, which are in the ideal generated by $X^q - Y^p$.

Question: a) An element r in a ring R of characteristic 5 satisfies $r^{999} = 0$, then find $n > 0$ such that $(1 + r)^n = 1$.

Solution: Take $n = 1000 = 10^3$, since the ring is of characteristic 5 we have $(1 + r)^{10^3} = 1 + r^{10^3} = 1$, since $r^{1000} = 0$.

Question: b) Let F be the two element ring. Find a reducible polynomial in $F[X]$ of smallest possible degree, which has no roots in F.

Solution: Take the polynomial to be $(X^2 + X + 1)^2$.

Question: c) Find all monic polynomials $g(X)$ in $\mathbb{Q}[X]$ such that when f is irreducible then so is $f(g(x))$.

Solution: It implies that $g(X)$ is irreducible and $g(X) - q$ is irreducible for all q rational. In particular we can choose $q = a_m$, where a_m is the constant term in $g(X)$. But $g(X) - a_m$ is $X g_1(X)$, so it is not irreducible. So there does not exists any such polynomial with non-zero constant terms. So g has $a_m = 0$ also $g(X)$ is irreducible. That gives us that $g(X) = X$.

Question: Show that upto isomorphism there are exactly 4 rings of cardinality 4. What about rings of cardinality 9?

<u>Solution</u>:

In a ring of order 4, we have $4.1 = 0$, so the characteristic is either 2 or 4. So for all element either $2a = 0$ or $4a = 0$. If $2a = 0$, then the ring is $\mathbb{Z}_2 \times \mathbb{Z}_2$ otherwise it is $\mathbb{Z}_4$. Now on each of then there are two ring operation, one is the natural one and the other one is trivial, i.e $(a, b)(c, d) = (ab, cd)$ or is equal to 0 for $\mathbb{Z}_2 \times \mathbb{Z}_2$. For $\mathbb{Z}_4$ we have the natural ring operation and the trivial one. So there are four rings of cardinality 4.

Same for rings of cardinality 9, either $\mathbb{Z}_3 \times \mathbb{Z}_3$ or $\mathbb{Z}_9$, and each having two ring operations.