Sheet 8 Solutions

Robert Kropholler

December 14, 2017

1. Show that the ideals (x) and (x, y) are prime ideals of $\mathbb{Q}[x, y]$. Further show that (x, y) is maximal while (x) is not.

   Proof. The map $\phi\colon \mathbb{Q}[x, y] \to \mathbb{Q}[y]$ given by evaluating at $x = 0$ is a homomorphism, it is easy to check that it is surjective and the kernel is (x). This is an integral domain but not a field, hence (x) is a prime ideal but not maximal.

   For the second part use the map $\psi\colon \mathbb{Q}[x, y] \to \mathbb{Q}$ by evaluating at $x = 0, y = 0$. This is a surjective homomorphism with kernel (x, y). This quotient is a field so this ideal is maximal and hence also prime. □

2. Let F be a finite field. Show that $F[x]$ has infinitely many prime elements. (Adapt Euclid's proof that $\mathbb{Z}$ has infinitely many primes.)

   Proof. Assume that there are only finitely many primes $p_1(x), \dots p_n(x)$ consider the polynomial $p_1 \dots p_n + 1$. This polynomial is not divisible by any of the polynomials p_i since if it were they would divide 1. Thus this is either prime or there was another prime element p. Either way our finite list cannot have been exhaustive. □

3. Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the polynomials with rational coefficients and integer constant term. This is a subring, you do not have to show this.

   (a) Show that the only units are ± 1.

   Proof. Consider two polynomials f, g such that $fg = 1$. We know that the constant terms of f and g multiply to give 1 and so they were ± 1. Let f have degree n and g have degree m. That is $f(x) = rx^n + \dot{\pm}1$ and $g(x) = sx^m + \dots \pm 1$. The product now has the term rsx^{n+m} and so is not a constant polynomial unless $n = m = 0$. □

   (b) Show that the irreducible elements are $\pm p$, for p a prime, and irreducible polynomials with constant term 1.

Proof. Any factorisation of an integer in $\mathbb{Z}$ is also a factorisation in R and vice versa. This shows that the only irreducible elements of R are $\pm p$ for p a prime. Similarly if a polynomial is reducible in $\mathbb{Q}[x]$, then we can reduce it in R. If a polynomial has a factorisation as two non-constant polynomials in R, then we also get a factorisation in $\mathbb{Q}[x]$.

If an irreducible polynomial $f(x)$ has constant term $a \neq 1$ then we can factor it as $a \cdot f'(x)$. This gives a reduction. Since any factorisation of an irreducible polynomial must be like this by the above, we see that irreducible polynomials with constant term ± 1 are still irreducible in R. □

(c) Show that x cannot be written as a product of irreducible elements. Deduce that R is not a UFD.

Proof. Assume x is a product of irreducibles $p_1, \dots p_n$ then the product of the constant terms is the constant term of x and is non-zero. □

(d) Show that (x) is not a prime ideal.

Proof. $x = 7x \cdot \frac{1}{7}$ and neither of these elements are in (x). □

(e) (Extra Credit) Describe the ring $R/(x)$.

Proof. The quotient is $\mathbb{Z} \otimes \mathbb{Q}/\mathbb{Z}$. The addition is pointwise and the multiplication is given by $(a, b)(c, d) = (ac, ad + bc)$. □

4. Show that the intersection of two submodules is a submodule and an ascending union of submodules is a submodule.

Proof. Let N and M be two submodules. Let $m, n \in N \cap M$ and $r \in R$. Since n, m are in the intersection we can see that $n + m$ is in M and in N. It is also clear the rm is in M and N. Thus this intersection is a submodule.

Let $A_1 \subset A_2 \subset \dots$ be an ascending chain. Consider elements a, b in the union. There is a k such that $a, b \in A_k$, thus we can work in this module and see that sums and multiples exist here to complete the proof. □

5. Let M be a module and N a submodule. The *annihilator of* N is the set $\{r \in R \mid rn = 0, \forall n \in N\}$, this is an ideal of R. Let I be an ideal of R. The *annihilator of* I is the set $\{m \in M \mid am = 0, \forall a \in I\}$, this is a submodule of M.

(a) Let $a_i > 1$. Find the annihilator of the $\mathbb{Z}$-module $\mathbb{Z}/a_1\mathbb{Z} \times \dots \mathbb{Z}/a_m\mathbb{Z}$.

Proof. We can see that the module $\mathbb{Z}/a_i\mathbb{Z}$ is annihilated by (a_i). Thus the module above is annihilated by the intersection $\cap_{i=1}^{m}(a_i) = (\text{lcm}(a_1, a_2, \dots a_m))$. □

(b) Find the annihilator of the ideal $2\mathbb{Z}$ in the above module.

Proof. We must consider all the elements of order 2. An element $(x_1, \dots x_m)$ has order 2 iff $2x_i$ is divisible by a_i for all i. This shows that $x_i = 0$ or $x_i = a_i/2$ this latter possibility only happens in the case when a_i is even. □

(c) Let $I \subset R$ be the annihilator of $N \subset M$ show that the annhilator of I contains N. Give an example where they are not equal.

Proof. Following the definitions it is clear that anything in N multiplied by and element of I is 0.

Consider $M = \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$. The annihilator of N is the ideal $I = 2\mathbb{Z}$ but the ideal I annihilates everything. □

(d) Let $N \subset M$ be the annihilator of $I \subset R$ show that the annhilator of N contains I. Give an example where they are not equal.

Proof. Following the definitions it is clear that anything in N multiplied by and element of I is 0.

Let $M = N = \mathbb{Z}/3\mathbb{Z}$. The annihilator of $2\mathbb{Z}$ is $\{0\}$ however the annihilator of $\{0\}$ is all of $\mathbb{Z}$. □

6. Let A be a $\mathbb{Z}$-module, let a be an element of A. Prove that the map $\phi_a \colon \mathbb{Z}/n\mathbb{Z} \to A$ given by $\phi_a(k) = ka$ is a well defined $\mathbb{Z}$-module homomorphism iff $na = 0$. Prove that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong \{a \in A \mid na = 0\}$, show this is the annihilator of the ideal $n\mathbb{Z}$.

Proof. If ϕ_a is a well defined homomorphims then $0 = \phi(0) = \phi(n) = na = 0$. For the other direction we can see that this function, if well defined, is additive and therefore respects the $\mathbb{Z}$ action. We must therefore check that it is well defined. Let $k \equiv l \mod n$ so $l = k + rn$. Then $\phi(k) = ka$ since $na = 0$ we see that $ka = ka + rna = la = \phi(l)$, so this map is well defined.

We can now define a map from $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$ to $\{a \in A \mid na = 0\}$ mapping ϕ_a to a. This map is well defined and surjective. Moreover $\phi_a + \phi_b = \phi_{a+b}$ so this is a homomorphism. It is surjective by the previous part and injective since if ϕ_a and ϕ_b have the same image, then $a = b$. □

7. Describe all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/24\mathbb{Z}$.

Proof. Using the question above we see that each homomorphism corresponds to an element a of $\mathbb{Z}/30\mathbb{Z}$ such that $24a \equiv 0 \mod 30$. A quick inspections shows these are the elements divisible by 4. Thus the homomorphism in notation above are $\phi_0, \phi_4, \phi_8, \phi_{12}, \phi_{16}, \phi_{20}$. □

8. Let $\mathrm{Tor}(M) = \{m \in M \mid \exists r \in R \setminus \{0\} \text{ such that } rm = 0\}$. Show that if R is an integral domain this is a submodule.

   Proof. It is clear that this set is closed under multiplication by elements of R we must now show that it is closed under addition. Let m, n be elements of $\mathrm{Tor}(M)$. There are elements r, s which are non-zero such that $rm = sn = 0$. We can then see that $rs(m+n) = rsm + rsn = 0 + 0 = 0$ and rs is non-zero as we are in an integral domain. □

9. Show that if $\phi : M \to N$ is an R-module homomorphism, then $\phi(\mathrm{Tor}(M)) \subset \mathrm{Tor}(N)$.

   Proof. If $x \in M$ is such that $x^k = 0$, then $0 = \phi(x^k) = \phi(x)^k$ so $\phi(x)$ is a torsion element. □

10. An R-module M is torsion if $M = \mathrm{Tor}(M)$. Show that all finite abelian groups are torsion $\mathbb{Z}$-modules. Find an infinite torsion $\mathbb{Z}$-module.

    Proof. Let G be a finite abelian group since G has finite order we know that every element has order dividing this and hence every element has finite order, hence this is a tosion module.

    Let $M = \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, every element of this group has order 2 or 1 and so it is torsion although it is clearly infinite. □

11. Let R be an integral domain, M a finitely generated torsion module. Show that the annhilator of M is not the zero ideal. Give an example of a not finitely generated torsion module whose annhilator is the zero ideal. (Hint: You can do it over $\mathbb{Z}$.)

    Proof. Let M be finitely generated by the set $S = \{s_1, \dots s_n\}$. Since M is a torsion module we can see that for each s_i there is a ring element r_i such that $r_i s_i = 0$. Let $r = r_1 \dots r_n$ and m and element of M. Since M is generated by the set S, we know that $m = a_1 s_1 + \cdots + a_n s_n$. We can also see that $rm = 0$ since $rs_i = 0$ for all i. Since we are in an integral domain, the element r is non-zero as the product of non-zero elements.

    For the last part consider the $\mathbb{Z}$-module $\bigoplus_{i=1}^{\infty} \mathbb{Z}/i\mathbb{Z}$ we can see that this is torsion since any element is contained in $\bigoplus_{i=1}^{n} \mathbb{Z}/i\mathbb{Z}$ for some n. However the annihilator would have to be contained in (i) for all i and is hence 0. □

12. An R-module M is called *irreducible* if $M \neq 0$ and if 0 and M are the only submodules. Show that M is irreducible iff $M \neq 0$ and M is cyclic with any non-zero element as a generator. Describe all irreducible $\mathbb{Z}$-modules.

Proof. Let M be an irreducible R module. Take a non-zero element m. The cyclic submodule m is non-zero and so must be all of M. Thus M is cyclic with any non-zero element as a generator.

For the other direction, assume that M is cyclic with any non-zero element as a generator. Let N be a non-zero submodule. Then N contains a non-zero element and hence contains the sub module generated by this element. Thus N is the whole module M.

When $R = \mathbb{Z}$ we can see that irreducible modules are cyclic groups and since a submodule is the same as a subgroup in this case we see that these must be simple abelian groups. These are exactly $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. □