Algebra HW5

Gandhar Kulkarni (mmat2304)

1

1. See that $bx - a \in \ker \pi$, since $b \cdot \left(\frac{a}{b}\right) - a = 0$. Therefore $(bx - a) \subseteq \ker \pi$. Now consider $f(x) \in R[x]$ where $f(x) \in \ker \pi$. We consider the polynomials $f(x)$ and $x - \frac{a}{b}$ as elements of $Q[x]$ the ring of polynomials with coefficients from the fraction field of R. Then this is a PID, which is why we can apply the division algorithm to see that $f(x) = q(x)\left(x - \frac{a}{b}\right) + c$, where $c \in Q, q(x) \in Q[x]$. Setting $x = \frac{a}{b}$ we get $c = 0$. Thus we have $f(x) = q(x)\left(x - \frac{a}{b}\right)$. We rewrite all polynomials are primitive polynomials in $R[x]$; thus we have $f(x) = a_1 \cdot f_0(x)$, $q(x) = a_2 \cdot q_0(x)$, and $x - \frac{a}{b} = b^{-1} \cdot (bx - a)$. Then we have $a_1 \cdot f_0(x) = (a_2 b^{-1}) q_0(x)(bx - a)$. We multiply on both sides by some $k \in R$ such that $ka_1 b \in R$ and $ka_2 \in R$ and the two are coprime. The constant cannot divide the polynomials as they are all primitive, hence we must have $ka_1 b | ka_2$, and by Gauss' lemma we can say that $f_0(x) | q_0(x)(bx - a)$, that is, $f \in (bx - a)$. Thus we have $\ker \pi = (bx - a)$.

2. Note that $(1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}) = 2 \cdot 2 = 4$, which means that R is not a UFD. Therefore the above result needn't apply. To show that the above result strictly does not apply, we need to find $f \in \ker \pi$ such that $f \notin (2x - (1 + \sqrt{-3}))$. See that $f(x) = x^2 - x + 1$ does the trick well. It is in fact the minimal polynomial, but it is not in $(2x - (1 + \sqrt{-3}))$. It is easy to prove, as the ideal of leading coefficients $R \cap (2x - (1 + \sqrt{-3})) = (2)$, and this clearly does not include the leading coefficient of $f(x)$. Thus $f \in \ker \pi \backslash (2x - (1 + \sqrt{-3}))$.

   The underlying reason for why this fails stems from the fact that the ring of integers of the number field $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{-3}]$; that is, the ring of integers is strictly larger than R as given in this problem. This has to do with the fact that $-3 \cong 1 \mod 4$, which introduces interesting additional algebraic integers into the number field.

2

1. Let us assume for the sake of contradiction that I has less than three generators. Then could have two generators, or even one. In case there is one generator, then let $I = (f) = (x, y, z)$. See that $\frac{F[x,y,z]}{(x,y,z)} \equiv F$, thus I is maximal, and hence prime. Thus f must be prime. Then we have $f | x$, which implies that f divides x, a prime itself, which is absurd. Hence no such f exists, and I cannot have just one generator.

   I is not generated, but it could be generated by two elements. If this is the case, let $I = (f_1, f_2)$. Then consider this expression modulo I^2. Note that I^2 gives us the module of all polynomials in R with degree greater than or equal to 2. Since I is maximal as an ideal in R, $\frac{I}{I^2}$ will be a $\frac{R}{I} \equiv F-$module, that is, a vector space. See that x, y, z reduced modulo I^2, are linearly independent, so this means that as a vector space $\frac{I}{I^2}$ has dimension ≥ 3. This naturally means that two generators will not be sufficient.

2. We know that all commutative rings have a maximal ideal, thanks to Zorn's lemma. Then we have for a commutative ring A the maximal ideal $\mathfrak{m}$, so we have $\frac{A[x,y,z]}{\mathfrak{m}} \equiv \left(\frac{A}{\mathfrak{m}}\right)[x, y, z] = F[x, y, z]$, where $F := \frac{A}{\mathfrak{m}}$ is a field. Note that $\mathfrak{m}A[x, y, z]$ is a maximal ideal in $R = A[x, y, z]$, and $I = (x, y, z)$ is a $R-$module. Thus we can say that $\frac{I}{\mathfrak{m}I}$ is a $F-$module. Now we need to see that x is not affected by reduction modulo $\mathfrak{m}I$. See that $x \in \mathfrak{m}I$ means that $x = \sum_{\text{finite}}(xf_1 + yf_2 + zf_3)$, where $f_1, f_2, f_3 \in (\mathfrak{m})[x, y, z]$. Then by putting $y = z = 0$, we get $x = \sum_{\text{finite}} xf_1(x) \implies \sum_{\text{finite}} f_1(x) = 1$. Comparing the constant terms, we must have a combination of scalars in $\mathfrak{m}$ that add up to 1. However, that would imply that $1 \in \mathfrak{m}$, which is absurd. Thus $x \notin \mathfrak{m}I$, and similarly for y and

z. Now we consider the map $\pi : I \to \frac{I}{\mathfrak{m}I}$ which is the canonical map. Then see that x, y, z are not affected by this map as previously shown. For any $h(x,y,z) = xh_1 + yh_2 + zh_3 \in I$, we have $\pi(h(x,y,z)) = x\bar{h_1} + y\bar{h_2} + z\bar{h_3}$. We have $\frac{I}{\mathfrak{m}I} \cong I$ as a $\frac{R}{\mathfrak{m}} = F[x,y,z]-$module.Using the previous result, we can say that this cannot have less than three generators, which gives us our answer.

3

Let $R = \frac{F[x,y]}{xy}$, and $I = (\bar{x}, \bar{y})$. Then

$$\frac{R}{I} \equiv \frac{\frac{F[x,y]}{(xy)}}{(\bar{x}, \bar{y})} \equiv \frac{F[x,y]}{(xy, x, y)} \equiv \frac{F[x]}{0 \cdot x, x} \equiv F,$$

which is a domain. Thus I is prime. To see that it is not principal, we assume for the sake of contradiction that $I = (f_0)$, where $f_0 \in F[x,y]$. Note that once seen modulo (xy), we have $\bar{f_0} = f_1(x) + f_2(y)$, where $f_1 \in F[x], f_2 \in F[y]$. If we say that $(f_0) = (\bar{x}, \bar{y})$, then we have $f_0 | x$ and $f_0 | y$. $f_0(x,y) = f_1(x) + f_2(y)$ must have degree less than or equal to 1, with no term of y, hence $f_2(y) = c_2$ and $f_1(x) = c_1 + dx$. Set $c = c_1 + c_2$, then see that we must have $x = t(c + dx)$ for some $t \in F[x,y]$. Comparing degrees, we must have $t \in F \backslash \{0\}$. Comparing the two sides, see that $c = 0, d = 1/t$ which is the only possibility. However, $x \nmid y$, so such a f_0 cannot exist. Thus I is not principal.

We know that prime ideals in R correspond to prime ideals in $F[x,y]$ that contain (xy). Let $\mathfrak{p}$ be the prime ideal in $F[x,y]$ containing (xy) and $\overline{\mathfrak{p}} = \pi(\mathfrak{p})$, where π is the natural map from $F[x,y]$ to R. Either $x \in \mathfrak{p}$ and $y \notin \mathfrak{p}$ or $x \notin \mathfrak{p}$ and $y \in \mathfrak{p}$ or $x \in \mathfrak{p}$ and $y \in \mathfrak{p}$. In the first case, see that $(F[x])[y]$ is a polynomial over a PID. From a previous assignment, we know that a prime ideal over such a ring would either be (0), $(f(y))$ for $f(y)$ irreducible in $(F[x])[y]$ or $(p, f(y))$ where p is prime in $F[x]$ and $f(y)$ is irreducible in $\frac{(F[x])[y]}{(p)}$. The first two cases are already principal, we need to see that the third case is also principal. x is a prime in $F[x]$. See that $f(y) = xg(x,y) + f_1(y)$ where $f_1(y)$ is irreducible in $F[x,y]/(x) = F[y]$. Then we have $\mathfrak{p} = (x, f_1(y))$. We have $\overline{\mathfrak{p}} = (x, \overline{f_1(y)})$. By our assumption $f_1(y)$ is an irreducible polynomial different from y, so its constant term is necessarily non-zero. Then we have in R, $x(\overline{f_1(y)}) = \overline{cx}$, where $c \in F$ is the constant term of the polynomial $f_1(y)$. Thus we have $c^{-1}cx \in (\overline{f_1(y)})$, thus $\overline{\mathfrak{p}} = (\overline{f_1(y)})$, a principal ideal.

The idea applies to the second case. In the third case, see that only the third type is possible. Thus we have $\mathfrak{p} = (x, f(y))$. Since $y \in \mathfrak{p}$, and $f(y)$ is irreducible, we must have $f(y) = y$. Then $\overline{f(y)} = y$, thus $\overline{\mathfrak{p}} = (x, y)$, which as discussed is the non-principal ideal.

Thus every other prime ideal is principal.

4

Let

$$A = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 5 & 5 & 4 & 4 \\ 6 & 7 & 7 & 8 \\ 10 & 10 & 9 & 9 \end{pmatrix}.$$

Through a myriad set of row and column operations shall we reduce our matrix A to form that will generate an alike cokernel. We shall use R_1, R_2, and R_3 to denote the rows, while C_1, C_2, and C_3 shall denote the columns of A. First we execute $C_2 \mapsto C_2 - C_1, C_4 \mapsto C_4 - C_3$. Then we execute $C_4 \mapsto C_4 - C_2$ to get

$$A' = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 5 & 0 & 4 & 0 \\ 6 & 1 & 7 & 0 \\ 10 & 0 & 9 & 0 \end{pmatrix}.$$

Execute $C_2 \mapsto C_2 - C_1, C_3 \mapsto C_3 - 2C_1$ to get

$$A'' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 5 & -5 & -6 & 0 \\ 6 & -5 & -5 & 0 \\ 10 & -10 & -11 & 0 \end{pmatrix}.$$

Execute $R_2 \mapsto R_2 - R_1, R_3 \mapsto R_3 - 6R_1$, and $R_4 \mapsto R_4 - 10R_1$. After this, execute $R_3 \mapsto R_3 - R_2$ and $R_4 \mapsto R_4 - 2R_2$ to get

$$A''' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -5 & -6 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Execute $R_2 \mapsto -R_2$, and $R_4 \mapsto R_4 - R_3$. After this execute $R_2 \mapsto R_2 - 6R_3$ to get

$$A'''' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

We are well aware that the cokernel is left unchanged due to our row and column operations. Thus it can be seen that the image of this matrix is $A''''(x_1 x_2 x_3 x_4)^T = (x_1 5x_2 x_3 0)$. Therefore the image is $\mathbb{Z} \oplus 5\mathbb{Z} \oplus \mathbb{Z} \oplus 0$. Then $\text{coker} A = \frac{Z^4}{\mathbb{Z} \oplus 5\mathbb{Z} \oplus \mathbb{Z} \oplus 0} = \frac{\mathbb{Z}}{5\mathbb{Z}}$.

5

1. Since $f \circ g = 0$, we have $f(g(p)) = 0 \forall p \in P$. Then we have $g(p) \in \ker f \forall p \in P \implies g(P) \subseteq \ker f$. Thus we can define $h : P \to \ker f$ as $h(p) = g(p)$. If another $h' : P \to \ker f$ exists such that $g = i \circ h'$, then we have $g = i \circ h = i \circ h'$. Since i is injective, for all $p \in P$ we have $i(h(p)) = i(h'(p)) \implies h(p) = h'(p)$, thus we have $h = h'$, proving the uniqueness of h.

2. Let $h(\bar{n}) = g \circ \pi^{-1}(\bar{n})$, for $\bar{n} \in \text{coker} f$. We propose that this is the desired map. We need to see that this map is well defined. $\pi^{-1}(\bar{n}) = n + f(M)$, for some $n \in N$. We need to see that the choice of representative does not matter. We can see that since g is $R-$linear we have $g(n + f(M)) = g(n) + g \circ f(M) = g(n) \in P$. Thus this map is well defined. To see that this map is unique, for another such map $h' : \text{coker} f \to P$ such that $g = h \circ \pi$, we have $g = h \circ \pi = h' \circ \pi$, which implies that $h = h'$ is surjective, where right cancellation is possible. Thus this map is unique.

6

We can see that $(0) \subseteq \ker f \subseteq \ker f^2 \subseteq \dots$ which is an ascending chain of submodules of M. This clearly must stabilise as the Noetherian condition is equivalent to the ascending chain condition. That is, for some $n \in \mathbb{N}$ we have $\ker f^n = \ker f^{n+1} = \ker f^{n+2} = \dots$. Now see that for some $m \in \ker f$ we have $f(m) = 0$. Since f is surjective, we can find a $m' \in M$ such that $f(m') = m$. Repeating this process, see that there must exist some $m_n \in M$ such that $f^n(m_n) = m$. Applying f on both sides, we have $f^{n+1}(m_n) = f(m) = 0$. Thus $m_n \in \ker f^{n+1} = \ker f^n$, we must have $f^n(m_n) = m = 0$. Thus m must necessarily be zero, meaning that a surjective endomorphism on a Noetherian module must necessarily be injective, and thus an isomorphism.