THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2024-25
Tutorial 10 solutions
28th November 2024

- The tutorial solutions are written for reference and proofs will be sketched briefly. You should try to fill in the details as an exercise. Please send an email to echlam@math.cuhk.edu.hk if you have any further questions.
- **Important: The extra content of this tutorial will not appear in the final exam.**

1. (a) Let R be a nonzero Noetherian ring, if R has no maximal ideal, then we can inductively find an increasing chain of ideals $I_1 \subset I_2 \subset ...$ such that I_k is strictly contained in I_{k+1}. This is because each I_k is not a maximal ideal, so it is strictly contained in some proper ideal I_{k+1}. However, this contradicts with the ascending chain condition of a Noetherian ring (see HW10 Q3).

   (b) Proof using (FBC): Let R be a PID, any ideal I is principal, so it is generated by one element, in particular it is finitely generated.

   Proof using (ACC): Let R be a PID, let $I_1 \subset I_2 \subset ...$ be an increasing chain of ideals in R. Then each $I_k = \langle a_k \rangle$ for some $a_k \in R$ such that $a_{k+1} | a_k$. Suppose that this chain of ideals does not terminates for some finite $n > 0$, then by replacing $\{I_n\}$ by a subsequence if necessary, we might assume that $a_{k+1} \mid a_k$ but a_k and a_{k+1} are not associate for all k (i.e. $a_k = b_k \cdot a_{k+1}$ for b_k not a unit. Note that this implies that a_1 can be written as a product of an arbitrarily large numbers of non-units. This contradicts with unique factorization of a_0. This is because the number of non-units factors appearing in the unique factorization of a_0 is constant.

   (c) Let k be a field, consider $k[x_1, x_2, ...]$ the polynomial ring on countably many variables. Note that $k[x_1, ..., x_n]$ is a UFD for any $n > 0$, since R is a UFD implies that $R[t]$ is a UFD. So for any polynomial f in $k[x_1, x_2, ...]$, it lies in the subring of $k[x_1, ..., x_n]$ for some large enough n, then f regarded as a polynomial in $k[x_1, ..., x_n]$ can be uniquely written as products of polynomials, up to units. Such unique product still remains to be unique in the original ring because polynomials involving the variable x_N for $N > n$ clearly does not appear in any factor of f.

   On the other hand, $k[x_1, x_2, ...]$ is no Noetherian. Because $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset ...$ is an increasing chain of ideals that does not terminate at finite $n > 0$.

   (d) Suppose that $\varphi : R \to R$ is a surjective homomorphism, consider $I_k = \ker \varphi^k$, then $I_1 \subset I_2 \subset ...$ is an increasing chain of ideals. So by Noetherian property, it must terminate for some $n > 0$. Then $\ker \varphi^n = \ker \varphi^{n+1}$. Now $\varphi^{n+1}(x) = 0$ implies that $\varphi^n(x) = 0$. Now suppose that $\varphi(x) = 0$, then by surjectivity $x = \varphi^n(y)$, so that $\varphi^{n+1}(y) = 0$, but this of course implies that $x = \varphi^n(y) = 0$.

2. (a) By Q1b, $\mathbb{Z}$ is Noetherian.

   On the other hand, the chain of ideals $J_1 \supset J_2 \supset ...$ defined by $J_k = 2^k\mathbb{Z}$ is a decreasing sequence of ideals which does not terminate at finite n. So $\mathbb{Z}$ is not Artinian.

(b) By Q1b, $k[t]$ is Noetherian.

Consider the decreasing chain $J_1 \supset J_2 \supset ...$ defined by $J_k = \langle t^k \rangle$. This never terminates for finite $n > 0$, so it is not Artinian.

(c) Note that we have a homomorphism $k \hookrightarrow k[t]/\langle t^n \rangle$, which realizes $k[t]/\langle t^n \rangle$ as a finite dimensional k-vector space. One can simply see that as vector spaces, $k[t]/\langle t^n \rangle \cong \mathrm{Span}_k(1, t, t^2, ..., t^{n-1})$. Then an ideal $I \subset k[t]/\langle t^n \rangle$ is a k-subspace, because for $a, b \in k$ and $x, y \in I$, $ax + by \in I$ by properties of an ideal. In particular, any decreasing chain of ideals is a decreasing chain of k-vector subspace in a finite dimensional vector space. Hence it must terminates for finite $n > 0$.

Remark: A commutative ring R together with a injective homomorphism $k \hookrightarrow R$ is called a commutative k-algbera. Via the inclusion, one realizes R as a k-vector space. Then what we have shown above is that a finite dimensional commutative k-algebra is always Artinian.

(d) Let R be an Artinian integral domain, pick any $x \in R \setminus 0$, then $\langle x \rangle \supset \langle x^2 \rangle \supset ...$ is a descending chain, so we have for large enough n, $\langle x^n \rangle = \langle x^{n+1} \rangle$. Therefore $x^n = x^{n+1}y$ for some y, so $x^n(1 - xy) = 0$, and we have $xy = 1$ by cancellation property of integral domains.

Remark: It turns out that every Artinian ring is Noetherian, but the converse is not true. This result is out of the scope of this course.

3. (a) First notice that both x^2 and x^3 are irreducible, since there are no degree 1 polynomial in R, so by a degree argument, they are both irreducible. Now x^6 can be factorize in two ways: $x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$ gives two ways of factorizing x^6 into irreducible elements, and these two factorizations do not differ by units. So R is not a UFD.

(b) Both x^2 and x^3 are not prime, as demonstrated by the above. x^2 divides $x^3 \cdot x^3$ but x^2 does not divide x^3. Likewise x^3 divides $x^2 \cdot x^4$, but it divides neither x^2 nor x^4.

(c) It is clear that the only divisors of x^2 are ± 1 and $\pm x^2$, similarly the only divisors of x^3 are ± 1 and $\pm x^3$. So $\gcd(x^2, x^3) = 1$, but clearly it is impossible to have $1 = p(x)x^2 + q(x)x^3$.

Remark: In an integral domain R, it is called a GCD domain if for every pair of x, y, a $\gcd(x, y)$ exists. It is called Bézout domain if gcd exists and it is always a linear combination $\gcd(x, y) = ax + by$, i.e. the Bézout's identity holds.

4. (a) Recall the ring $\mathbb{Z}[\sqrt{-5}]$ we saw from the lecture, we have seen that it is not a UFD because there are two ways of factorizing 9: $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$. Inspired by this, we can try to argue that $a = 3(2 + \sqrt{-5})$ and $b = 9$ do not have a gcd. One can make use of property of the norm function $N(a + b\sqrt{-5}) = a^2 + 5b^2$. (Note that it is not Euclidean norm, it is just a function.) If $x|y$ then we have $N(x)|N(y)$. One can write down all the factors of a, b respectively and note that there are no greatest common divisors.

More concretely, we have $N(9) = 81$, so its divisors must have norm equals to $1, 3, 9, 27, 81$. Notice that if $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = 1$ then $a + b\sqrt{-5}$ is a unit. So we only have to consider cases when norm is equal to $3, 9$ or 27. Notice that $a^2 + 5b^2 = 3$ or 27 have no solutions by reducing the equation

$\mod 5$. So any nontrivial divisor of 9 must have norm 9. Then it is clear that its nontrivial divisor must be $\pm 3, \pm(2+\sqrt{-5}), \pm(2-\sqrt{-5})$. Similarly one can deduce that $3(2+\sqrt{-5}$ has nontrivial divisor $\pm 3, \pm(2+\sqrt{-5})$. It is clear that there is no greatest common divisor since 3 and $2+\sqrt{-5}$ are not associate.

(b) Let R be a UFD, and $x, y \in R$, we can write $x = u_x \cdot x_1 ... x_n$ and $y = u_y \cdot y_1 ... y_m$ where u_x, u_y are units and x_i, y_j are irreducible elements. Up to permutation and factoring units, we can rearrange the x_i's and y_i's so that $x_i = y_i$ for $i = 1, ..., k$. This is because if two irreducible elements a, b have non-units common factors, then they are both associate to that factor. Otherwise if their common factors are all units, then $\gcd(x, y) = 1$ by definition. Then the claim is that $\gcd(x, y) = x_1 ... x_k = y_1 ... y_k$. To see why, suppose d is a common factor of x, y, then writing $d = u_d \cdot d_1 ... d_l$, by unique factorization, we must have for each i that $d_i \sim x_j$ for some j and $d_i \sim y_{j'}$ for some j'. Since $x_j \sim y_{j'}$, we can always take $1 \leq j = j' \leq k$. By induction, we can deduce that $d | x_1 ... x_k$. So it is indeed the gcd.

(c) An element m' is called a common multiple of x, y if $m' = ax = by$ for some a, b. Then an lcm of x, y (if exist) is a common multiple m of x, y such that m divides all common multiples of x, y.

Write $d = \gcd(x, y)$. Using the notation of part (b), we are going to prove that the following is an lcm of x, y: $m = (x_1 ... x_k)(x_{k+1} ... x_n)(y_{k+1} ... y_m)$. Then it is clear that $dm = xy$ up to units. Suppose m' is a common multiple of x, y, again we look factorization of m' into irreducibles $m' = u r_1 ... r_p$. Again up to units, it contains all the x_i as factors since $x | m'$. We may assume that $x_i = r_i$ for $i = 1, ...n$. Then since $y | m'$ and $y_j \not\sim x_i$ for $j > k$. We must have $y_j | r_{n+1} ... r_p$ for $j > k$. So again up to units, we can write $y_{k+j} = r_{n+j}$. In other words, $m' = u(x_1 ... x_n)(y_{k+1} ... y_m) ... r_p$, so $m | m'$. So m is an lcm of x, y.

5. Since D is a PID, the maximal ideal $\mathfrak{m} = \langle t \rangle$ (such t is called a uniformizing parameter). For any $x \in D \setminus \{0\}$, since $t^0 = 1$ always divides x, there is some largest non-negative integer k such that $t^k | x$. Then $\langle x \rangle \subset \mathfrak{m}^k = \langle t^k \rangle$. We define $\nu(x) = k$.

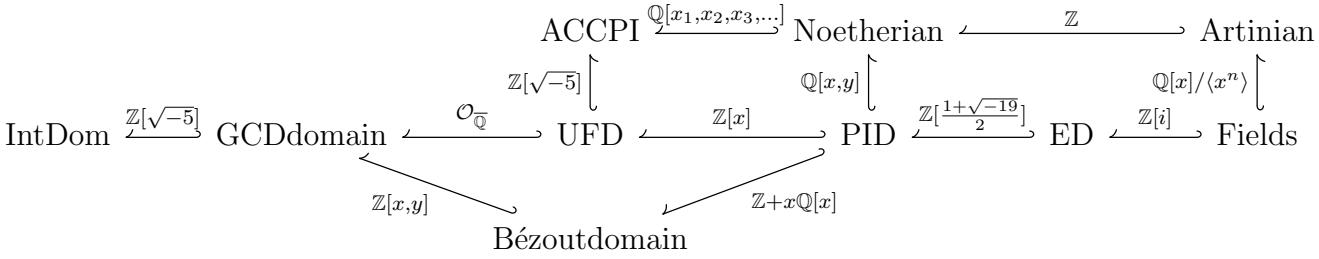
   In fact, we have $\langle x \rangle = \langle t^k \rangle$, i.e. $x \sim t^k$. This is because $x = a t^k$, since k is the largest, we know $t \nmid a$. In other words, $a \notin \langle t \rangle = \mathfrak{m}$. But every non-unit element must be contained in some maximal ideal by Zorn's lemma, which in the case of D being a DVR, must be $\mathfrak{m}$. So a, lying outside $\mathfrak{m}$, must a unit. In particular, this shows that every element in a DVR can be expressed as $x = a t^i$ for some unit a and $i \geq 0$.

   Now apply the above result to $x, y \in D$, $y \neq 0$. We may write $x = a t^i$ and $y = b t^j$ for units a, b. Then $\nu(y) = j$. If $i \geq j$, then we may take $q = a b^{-1} t^{i-j}$, so $x = qy$ and so $r = 0$. Otherwise $i < j$, so we might take $q = 1$ and so $r = x - y = t^i(a - b t^{j-i})$. Since t^i is the largest power dividing r, so $\nu(r) = i < j = \nu(y)$ as desired.

   Finally, $xy = ab t^{i+j}$ clearly satisfies $\nu(x) \leq \nu(xy)$, as $i, j \geq 0$.

6. Using the norm function $N(a + bi) = a^2 + b^2$. We know that if $a + bi$ divides 13, then $N(a + bi) = a^2 + b^2$ divides $N(13) = 169$. And since 13 is real, if $a + bi$ is a factor, then so is $a - bi$. In other words, we must have $a^2 + b^2 = 13$. This gives $a = 2, b = 3$ or $a = 3, b = 2$. So we can factorize $13 = (3 + 2i)(3 - 2i)$. Notice that this is the same as $(2 + 3i)(2 - 3i)$ since they are associate $i(3 - 2i) = 2 + 3i$. One can see that $2 + 3i$ is prime since $N(2 + 3i) = 13$ is prime.

7. All the previous exercises culminated to the following. Here the arrows mean we have strict inclusions between each class of objects. Above each arrow, there is a counterexample of an object that belongs to the larger class but not the smaller one, e.g. $\mathbb{Z}[i]$ is a Euclidean domain but not a field.



(a) There are a lot to cover here. Let's briefly go over what the special rings are. $\mathbb{Z} + x\mathbb{Q}[x]$ is just the ring of polynomial in $\mathbb{Q}$ so that the constant coefficient $a_0 \in \mathbb{Z}$. It is not a PID for similar reason as $\mathbb{Z}[x]$.

(b) $\mathbb{Z}[x, y]$ is not a Bézout domain since x^2y, xy^2 has gcd given by xy. But clearly you cannot take linear combinations of higher degree polynomial to obtain lower degree ones. It is a GCD domain since it is a UFD.

(c) For $\mathbb{Q}[x_1, x_2, x_3, ...]$ see Q1c.

(d) A ring R is a UFD if and only if it is a GCD domain and satisfies ACCPI.

(e) A commutative ring R is a Bézout domain if and only if all finitely generated ideals are principal. In a GCD domain (and hence for also for Bézout domains), any irreducible element is prime (try to prove it!). Hence, if R is a Bézout domain, then the following are equivalent: (i) R is a UFD, (ii) R is PID, (iii) R satisfies ACCPI, (iv) R is Noetherian.

(f) For $\mathbb{Q}[x]/\langle x^n\rangle$ see Q2c.

(g) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID that is not a Euclidean domain. It is not easy to see this. Such rings are called quadratic integers, they are analogous to integers in $\mathbb{Q}$ that lives in a field extension of $\mathbb{Q}$. They were a important part of 19th century number theory, heavily studied by Gauss, Kummer and Dedekind. These rings, called ring of integers are always a Dedekind domain, which roughly are domains where we have factorization of ideals into products of prime ideals. One remarkable property of Dedekind domain is that it is a UFD iff it is a PID iff it is a GCD domain. Studying whether a Dedekind domain is a PID is closely related to a notion called ideal class group, which is an important notion in algebraic number theory.

(h) $\mathbb{Q}[x, y]$ is not a PID since $\langle x, y\rangle$ is not principal. It is Noetherian by a result of Hilbert. The Hilbert's basis theorem asserts that if R is a Noetherian ring, then $R[x]$ is again Noetherian.

(i) $\mathcal{O}_{\overline{\mathbb{Q}}}$ sometimes also denoted as $\overline{\mathbb{Z}}$ is called the algebraic integers. It contains all roots of *monic* polynomial $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, i.e. polynomial with integer coefficients such that the leading coefficient is 1. It is not trivial at all that it forms a GCD domain (actually a Bézout domain). But we can see that it is not a UFD since in fact it has no irreducible elements: if $z \in \overline{\mathbb{Z}}$, say $p(z) = 0$ for some monic $p \in \mathbb{Z}[x]$, then $\sqrt{z}$ satisfies $p(x^2) \in \mathbb{Z}[x]$ which is also monic, so $\sqrt{z} \in \overline{\mathbb{Z}}$ is a

divisor of z. Note that z is a unit if the polynomial $p(x)$ has constant coefficient 1, so z is a unit if and only if $\sqrt{z}$ is a unit. This implies that if z is not a unit, it is never irreducible. Thus, there is no unique factorization.