Selected Solutions for Tutorial 5 - Algebra 2019

(1) Show that $\mathbb{Z}$ is a PID, UFD, GCD domain, and Euclidean domain. Try to consider the properties you used in order to find a hierarchy between these classes.

GCD Domains $\supset$ UFDs $\supset$ PIDs $\supset$ Euclidean Domains $\supset$ Fields. $\mathbb{Z}$ is not a field, but it is a Euclidean domain.

(2) Let $\mathcal{R} = \{f : \mathbb{C} \to \mathbb{C} \mid f \text{ is entire}\}$ be the ring of entire functions. Fill out some the following table with Yes or No, explaining each entry.

	GCD Domain	UFD	PID	Euclidean Domain
$\mathbb{Z}[X]$	Yes	Yes	No	No
$\mathbb{Z}_4$	No	No	No	No
$\mathbb{Z}[\mathrm{i}]$	Yes	Yes	Yes	Yes
$\mathbb{R}[X, Y]$	Yes	Yes	No	No
$\mathcal{R}$	Yes	No	No	No
$\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$	Yes	Yes	Yes	No

Ideas behind proofs:

- $\langle 2, X\rangle$ is an ideal in $\mathbb{Z}[X]$, but it cannot be principal. Alternatively, X is irreducible in $\mathbb{Z}[X]$, so if $\mathbb{Z}[X]$ were a PID, $\mathbb{Z}[X]/\langle X\rangle$ would have to be a field; it is $\mathbb{Z}$, which is not a field.
- $2 \times 2 = 0$ in $\mathbb{Z}_4$, so it is not even an integral domain. All of these must be integral domains.
- $\mathbb{Z}[\mathrm{i}]$ has one of the nicest non-trivial Euclidean division algorithms and a detailed Wikipedia page on it.
- If L is a UFD, then so too is $L[X]$. Since $\mathbb{R}$ is a field, it is a UFD, so $\mathbb{R}[X]$ is a UFD. But then $\mathbb{R}[X, Y] = \mathbb{R}[X][Y]$ (by definition) is also a UFD.
- To see that $\mathbb{R}[X, Y]$ is not a PID, consider the ideal $\langle X, Y\rangle$ and suppose it is generated by some polynomial $p(X, Y)$. Since $X, Y \in \langle X, Y\rangle$, $p(X, Y)$ must divide X and Y, so it must be a constant. But then $p(X, Y) \notin \langle X, Y\rangle$, which is a contradiction. Alternatively, recall (?) that $F[X]$ is a PID if and only if F is a field; $\mathbb{R}[X]$ is not a field since X is not invertible in $\mathbb{R}[X]$.
- You are not expected to know about entire functions (functions that are smooth on $\mathbb{C}$). However, if you've taken complex analysis, you may be interested to know that the primes in $\mathcal{R}$ are the linear polynomials

$(x-c)$ with $c \in \mathbb{C}$ (the set of primes is isomorphic to $\mathbb{C}$)! Given $f, g \in \mathcal{R}$, let $h(x) = \prod_{a:f(a)=g(a)=0}(x-a)$. Then $\gcd(f,g) = h$. On the other hand, the entire function $\sin(x)$ has infinitely many zeroes, so cannot be uniquely factorised as a product of finitely many primes. Thus, $\mathcal{R}$ is not a UFD.

- The PID $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ is technically in this course, but it would be cruel of us to put it on the exam (without heavy guidance). To see that it is not a Euclidean domain, note that $\gcd(1+\sqrt{-19}, 4) = 2$ but there is no way to obtain this from the Euclidean algorithm; indeed, there are no $q, r \in \mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ such that $1+\sqrt{-19} = 4q + r$. The "inspiration" required to find this example is quite technical, and so too is the proof that $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ is actually a PID.
- What's interesting is that $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ is a PID but not a Euclidean domain exactly when $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

(3) Use the Euclidean algorithm to find inverses of some elements in $\mathbb{Z}_5[\mathrm{i}]$ and $\mathbb{Z}_2[X]/\langle X^3 + X + 1\rangle$.

(4) Show that 9 is reducible in $\mathbb{Z}[\sqrt{-5}]$, and hence show that 3 is not prime (what are the units in $\mathbb{Z}[\sqrt{-5}]$? This may be worth proving).

The first part of this question is either ridiculously easy or misleading. In any case, define a norm by $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Then, if x is a unit in $\mathbb{Z}[\sqrt{-5}]$, $N(x) = 1$ (If $xy = 1$, $N(x)N(y) = N(xy) = N(1) = 1$, but $N(x), N(y)$ must be positive integers), so $x = \pm 1$. Now, $3 | 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, but 3 does not divide either of these factors, so it cannot be prime (use norm arguments).

(5) Is $\mathbb{Q}$ a free module over $\mathbb{Z}$?

It is not a free module, since it does not have a basis. Suppose, for the sake of contradiction, that it did have a basis. If such a basis had one element, say $v = p/q \in \mathbb{Q}$ with $\gcd(p,q) = 1$, then $p/(2q) \in \mathbb{Q}$ but $p/(2q) \notin \operatorname{span}_{\mathbb{Z}}\{v\}$, so our apparent basis does not span $\mathbb{Q}$ over $\mathbb{Z}$ and we have a contradiction. Now, if we suppose there is a basis with at least 2 elements, then we would lose linear independence, since any two rational numbers are linearly dependent over $\mathbb{Z}$.