Assignment 4, Math 4GR3
Due Apr. 1, uploaded to Avenue

1. There is a PID which is not a Euclidean domain. An explicit example is $Z[\theta]$ where
$$\theta = \frac{1}{2} + \frac{\sqrt{-19}}{2}.$$
This requires some fussy work and turns out to be more than I want to put on an assignment. However, on the honour system, I ask you to look at some presentations of this online. Here is a write-up by Conan Wong who was at UBC:

   www.m-hikari.com/imf/imf-2013/29-32-2013/wongIMF29-32-2013.pdf

   He points to other sources in the literature. The harder part is showing that this example is a PID.

2. We will show that every field is contained in an algebraically closed field.

   (a) Fix a field F and consider the set A of all polynomials in $F[x]$ which are irreducible over F. Introduce a variable x_f for every $f \in A$ and let I be the ideal generated by all $f(x_f)$ in the ring $R = F[x_f : f \in A]$ which is the ring of polynomials with variables x_f for $f \in A$. Show that I is not equal to R and then take a maximal ideal $J \subset R$ which contains I (for purists, this step requires Zorn's Lemma but just assume it; the main point is that I is a proper ideal). Note that R/J is a field and show that every polynomial over F has a root in R/J.

   Solution: As suggested, if we show that I is a proper ideal then we can find a field extension of F in which every irreducible polynomial over F has a solution. To see that I is proper, it is enough to show that $1 \notin I$. The general form of an element of I is
$$g_1 f_1(x_{f_1}) + \ldots + g_n f_n(x_{f_n})$$
   where $g_1, \ldots, g_n \in R$ and $f_1, \ldots, f_n$ are irreducible over F. Such an element can never equal 1. To see this, suppose that K is an extension of F in which $a_1, \ldots, a_{n-1}$ are solutions of $f_1, \ldots, f_{n-1}$ respectively. If this element was equal to 1 then if $a_1, \ldots, a_{n-1}$

were substituted for $x_{f_1}, \ldots, x_{f_{n-1}}$ we would get the equation over K:

$$g_n(a_1, \ldots, a_{n-1}, x_{f_n}) f_n(x_{f_n}) = 1.$$

But the right-hand side of this equation is a constant and the left-hand side is a non-trivial polynomial. So this cannot happen. We conclude that I is proper and if J is some maximal ideal in R which contains I then R/J is a field extension of F in which every irreducible polynomial over F has a solution.

(b) Let $F_0 = F$. Assume we have defined F_n and let F_{n+1} be defined as in part (a) starting with F_n in place of F. Let $K = \bigcup_n F_n$. Show that K is algebraically closed.

Solution: Suppose that one has a non-constant polynomial $f(x)$ over K. Since f has only finitely many coefficients, there is some n such that f's coefficients are all in F_n. By factoring f over F_n if necessary, we can assume that f is irreducible over F_n and by construction, f has a solution in F_{n+1}. So we can solve f in K. We conclude that K is algebraically closed.

3. Chap. 18, #5: We show that every prime element of an integral domain R is irreducible. Suppose that $p \in R$ is prime and that $p = ab$. Then p divdes ab and so by primeness, p divides a or b. Without loss, assume that $a = pc$. Then we have $p(cb) = p$. Since $p \neq 0$, we have $cb = 1$ which means that b is a unit.

4. Chap. 18, #11: $Z[\sqrt{-2}]$ is a subring of the complex numbers and the complex numbers is a field. So $Z[\sqrt{-2}]$ is an integral domain. If $a + b\sqrt{-2}$ is in $Z[\sqrt{-2}]$ and at least one of a or b is not zero then

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2}.$$

Since a and b are integers, we have $|a|, |b| \leq a^2 + 2b^2$. In order that the inverse also be in $Z[\sqrt{-2}]$, we would need $|a| = a^2$ and $b = 0$ i.e. $a = \pm 1$ and $b = 0$ so the only units in $Z[\sqrt{-2}]$ are ± 1. The fraction field of $Z[\sqrt{-2}]$ is $Q[\sqrt{-2}]$. Indeed since Z is a subfield of $Z[\sqrt{-2}]$ we must have Q in the fraction field and $\sqrt{-2}$ must be in the fraction field as well. Since $Q[\sqrt{-2}]$ is a field, it is the smallest field containing $Z[\sqrt{-2}]$ and hence is the fraction field.

Now let's show that $Z[\sqrt{-2}]$ is a Euclidean domain with valuation $\nu(a+b\sqrt{-2}) = a^2 + 2b^2$. This is close in style to example 18.20 in the text. It is clear that the values of ν are non-negative integers. We also have, for a, b, c and d in Z with at least one of c or d not 0

$$(a+b\sqrt{-2})(c+d\sqrt{-2}) = ac - 2bd + (ad+bc)\sqrt{-2}$$

and so the valuation of the product is

$$(ac-2bd)^2 + 2(ad+bc)^2 = a^2(c^2+2d^2) + 2b^2(2d^2+c^2) \leq a^2 + 2b^2$$

So $\nu(a+b\sqrt{-2}) \leq \nu((a+b\sqrt{-2})(c+d\sqrt{-2}))$.
Finally, suppose that we are given $a+b\sqrt{-2}, c+d\sqrt{-2} \in Z[\sqrt{-2}]$, both not zero. Then we can write

$$\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{ac+2bd+(ad+bc)\sqrt{-2}}{c^2-2d^2}$$

and this latter expression can be written as

$$(m+n\sqrt{-2}) + (s+t\sqrt{-2})$$

where m and n are integers and s, t are rational numbers of size less than or equal to $1/2$; m and n are the closest integers to the fractions appearing above. We would then have that $\nu(s+t\sqrt{-2}) \leq 1/4 + 1/2 = 3/4$. From this we conclude that

$$a+b\sqrt{-2} = (m+n\sqrt{-2})(c+d\sqrt{-2}) + (s+t\sqrt{-2})(c+d\sqrt{-2}).$$

Since $a+b\sqrt{-2}$ and $m+n\sqrt{-2}$ are both in $Z[\sqrt{-2}]$,
$(s+t\sqrt{-2})(c+d\sqrt{-2})$ is as well. Furthermore,

$$\nu((s+t\sqrt{-2})(c+d\sqrt{-2})) \leq \frac{3}{4}\nu(c+d\sqrt{-2})$$

which shows that $Z[\sqrt{-2}]$ is a Euclidean domain.

5. Chap. 18, #19 Show that if an integral domain is Artinian (satisfies the descending chain condition) then it is Noetherian (satisfies the ascending chain condition). This is a bit of a trick question: the fact

is that every Artinian ring is Noetherian but this requires some effort to prove. The assumption that we have an integral domain actually gives that any Artinian integral domain is a field! Take $a \neq 0$ in some Artinian integral domain R and form the descending chain $R \supseteq Ra \supseteq Ra^2 \supseteq \ldots Ra^n \supseteq \ldots$ Since R is Artinian, for some n, $Ra^n = Ra^{n+1}$. This means that for some $b \in R$, we have $ba^{n+1} = a^n$ or rewriting, $(ba-1)a^n = 0$. So $ba = 1$ and this shows that a is a unit. Since a was arbitrary, R is a field (and hence is Noetherian).

6. Chap. 22 #8 The two rings indicated are fields since the ideals being quotiented by are generated by irreducible polynomials. The fields both have size 8 and since there is only one field of size 8 up to isomorphism, these two fields are isomorphic.

7. Chap. 22, # 12 Show that no finite field is algebraically closed. Suppose that F is a finite field with elements $a_1, \ldots, a_n$. Form the polynomial

$$1 + \prod_{i=1}^{n}(x - a_i).$$

This polynomial has no solution in F and so F is not algebraically closed. (This proof is due to Euclid who didn't know what an algebraically closed field was!)

8. Chap. 22, # 21 Show that the map $\alpha \mapsto \alpha^p$ is an automorphism of order n for $GF(p^n)$.

That it is a ring homomorphism requires noticing that

$$(x+y)^p = x^p + y^p \text{ and } (xy)^p = x^p y^p$$

for all $x, y \in GF(p^n)$ because the characteristic is p. To see that this is an automorphism, it suffices to see that it is injective since the field is finite. If $x^p = y^p$ then again, because of the characteristic, $(x-y)^p = 0$ which implies that $x = y$. Since in $GF(p^n)$, all elements satisfy $x^{p^n} = x$, we see that the order of this automorphism is at most n. But if the order of the automorphism is m then we would have $x^{p^m} = x$ for all $x \in GF(p^n)$ which would mean that $x^{p^m} - x$ would have at least one root with multiplicity larger than one which is not true. So the order of the Frobenius automorphism is n. In fact, the Frobenius automorphism generates the automorphism group of $GF(p^n)$ and so the automorphism group is isomorphic to Z_n.