HOMEWORK 3

Due date: Tuesday of Week 4

Exercises: 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.9, 3.1, 3.2, 3.4, 3.6, pages 379-380 of Artin's book.

Hint for Exercise 2.10: Let $f = \sum_{n\geq 0} a_n x^n \in \mathbb{R}[[x]]$. If $a_0 \neq 0$, show that f is a unit in $\mathbb{R}[[x]]$. Exercise 3.4 is probably not so easy. You can use the fact that $\mathbb{C}[x, y, z, w]$ is a UFD and thus one can define gcd there. These facts are proved in the following problems.

Problem 1. *Let R be an integral domain and let $p \in R$ be a prime element. Show that p is irreducible.*

(Recall that: p is prime means that p is not a unit and if $p|ab$, then $p|a$ or $p|b$; p is irreducible means that p is not a unit and it cannot be factorized further, namely, if $p = ab$ for $a, b \in R$, then one of a, b is a unit.)

Let R be an integral domain and let F be its fractional field. An element $\alpha \in F$ is called integral over R if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$. The ring R is called **integrally closed** if for any $\alpha \in F$ integral over R, we have $\alpha \in R$.

Problem 2.
(1) *Show that $\mathbb{Z}$ is integrally closed.*
(2) *Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Its fractional field is*
$$F = \mathbb{Q}(\sqrt{-3}) = \left\{a + b\sqrt{-3} : a, b \in \mathbb{Q}\right\}.$$
Show that $\omega := \frac{-1+\sqrt{-3}}{2} \in F$ is integral over R but not in R. Thus R is not integrally closed.

Problem 3.
(1) *Let R be a UFD, show that R is integrally closed. Conclude that the ring $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. Find an irreducible element in $\mathbb{Z}[\sqrt{-3}]$ such that it is not prime.*
(2) *Let $\omega := \frac{-1+\sqrt{-3}}{2}$. Show that the ring $R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ is a Euclidean domain and thus it is a UFD.*

Hint for part (2): The proof is similar to the case that $\mathbb{Z}[i]$ is a Euclidean domain.

Let R be a ring. Given two elements $a, b \in R$. An element $d \in R$ is called a greatest common divisor (gcd) of a and b if it satisfies the following two conditions:
(1) $d|a, d|b$;
(2) if $x \in R$ is an element such that $x|a, x|b$, then $x|d$.

If such a d exists, and $u \in R^\times$, then ud also satisfies the above conditions. Conversely, if d, d' both satisfy the above gcd conditions, then there exists a unit $u \in R^\times$ such that $d' = ud$. To avoid such ambiguity, we use $gcd(a, b)$ to denote the principal ideal (d) if d satisfies the above condition and call this principal ideal the greatest common divisor of a and b.

Note that $gcd(a, b)$ in general is not the ideal (a, b) (which always means the ideal generated by a and b, namely $(a, b) = \{ax + by : x, y \in R\}$). For example, in the ring $\mathbb{C}[x, y]$, we have $gcd(x, y) = 1$, but $(x, y) \neq (1)$. Actually, $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$.

An integral domain R is called a **GCD domain** if for any $a, b \in R$, $gcd(a, b)$ exists.

Problem 4. *Let R be a GCD domain.*
(1) *Suppose $gcd(x, y)$ exists. Show that $(x, y) \subset gcd(x, y)$. In particular, if $(x, y) = 1$, then $gcd(x, y) = 1$. Note that the converse is not true by the above example.*
(2) *Let $a_1, \ldots, a_n \in R$. Show that there exists an element $d \in R$ such that (a) $d|a_i, \forall i$, and (b) if $x \in R$ such that $x|a_i, \forall i$, then $x|d$. This d is called the gcd of $a_1, \ldots, a_n$ and we denote it (or the principal generated by it) by $gcd(a_1, \ldots, a_n)$.*

(3) *Show that* $gcd(gcd(a,b),c) = gcd(a, gcd(b,c)), \forall a,b,c \in R$.
(4) *Suppose that* $gcd(a,b) = 1$ *for* $a,b \in R$. *Show that* $gcd(a^n, b) = 1$ *for any* $n \geq 1$.

In class, we showed that a PID is a GCD domain.

Problem 5. (1) *Show that a UFD is a GCD domain.*
(2) *Show that a GCD domain is integrally closed.*

Hint for (1): this gcd is what you learned from elementary school. (2), this proof is similar to Problem 3. You might have to use $gcd(a^n, b) = gcd(a, b)$ for $a, b \in R$, a GCD domain.

Thus we have the inclusions

$$ED \subset PID \subset UFD \subset GCD\ domain \subset integrally\ closed\ domain.$$

In the following several problems, we will show that if R is a UFD, then $R[x]$ is also a UFD. The proof is basically parallel to the case $\mathbb{Z}[x]$ as we did in class. Let R be a UFD. Given a polynomial $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, define $c(f) := gcd(a_1, \ldots, a_n)$. Note that $c(f)$ is well-defined up to associates. A polynomial $f \in R[x]$ is called **primitive** if $c(f) \sim 1$. Let F be the fractional field of R.

Problem 6. *Let* R *be a* UFD. $f, g \in R[x]$. *Show that* fg *is primitive iff* f *and* g *are both primitive.*

See Proposition 12.3.4 (b) for the case when $R = \mathbb{Z}$.

Problem 7. *Recall that* R *is a UFD and* F *is its fractional field.*

(1) *Show that every polynomial* $f \in F[x]$ *can be written as* $f = cf_0$ *with* $c \in F$ *and* $f_0 \in R[x]$ *is primitive. Moreover, if* $cf_0 = c'f_0'$ *with* $c, c' \in F', f_0, f_0' \in R[x]$ *primitive, show that there exists a unit* $u \in R^\times$ *such that* $c' = cu, f_0' = u^{-1}f_0$.
(2) *Show that* $c \in R$ *iff* $f \in R[x]$. *Moreover,* $f \in R[x]$, *then* $c \sim c(f)$.
(3) *Suppose* $f, g \in R[x]$ *are two primitive polynomials. If* $f = \alpha g$ *for some* $\alpha \in F^\times$, *show that* $\alpha \in R^\times$.

This is Lemma 12.3.5 when $R = \mathbb{Z}$.

Problem 8. *Let* R *still be a UFD and* F *be its fractional field.*

(1) *Let* $f \in R[x]$ *with* $\deg(f) > 0$. *If* f *is irreducible in* $R[x]$, *show that* f *is irreducible in* $F[x]$.
(2) *Show that* $f \in R[x]$ *is irreducible iff* f *is a prime element in* R *or a primitive polynomial that is irreducible in* $F[x]$.
(3) *Show that every irreducible element in* $R[x]$ *is a prime element.*

This is Proposition 12.3.7 when $R = \mathbb{Z}$.

Problem 9. *Let* R *be a UFD. Show that* $R[x]$ *is a UFD.*

This is Theorem 12.3.10.