Cavallaro, Jeffery
Math 221b
Homework #4

1). Determine the units in $(\mathbb{Z}/4\mathbb{Z})[x]$

We know that $(\mathbb{Z}/4\mathbb{Z})^{\times} = \{a + 4\mathbb{Z} \mid (a, 4) = 1\} = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$: Since addition and multiplication are by representatives, for convenience, we can work in arithmetic $\pmod 4$ for the coefficients.
Assume $f(x) \in (\mathbb{Z}/4\mathbb{Z})^{\times}$. The there exists $g(x) \in (\mathbb{Z}/4\mathbb{Z})^{\times}$ such that:

$$f(x)g(x) = 1$$

Thus, $a_0 = 1$ and all other $a_k = 0$.
The only possibilities for $a_0 = 1$ are $1 \cdot 1$ and $3 \cdot 3$.

Let $f(x) = 1 + af_1(x)$ where $f_1(x) \in (\mathbb{Z}/4\mathbb{Z})[x]$ and
let $g(x) = 1 + bg_1(x)$ where $g_1(x) \in (\mathbb{Z}/4\mathbb{Z})[x]$ and
AWLOG that the coefficients of $f_1(x)$ and $g_1(x)$ are relatively prime - otherwise factor out any common factors.
$f(x)g(x) = 1 + af_1(x) + bg_1(x) + abf_1(x)g_1(x) = 1$
The only possibilities that allow the last term to drop out occur when:

a). $a = 0$ or $b = 0$

b). $a = b = 2$

If $a = 0$ then b must also be 0 so that the two middle terms drop out. $a = b = 2$ works as long as $f_1(x) = g_1(x)$.

Now, let $f(x) = 3 + af_1(x)$ and $g(x) = 3 + bg_1(x)$.
$f(x)g(x) = 1 + 3af_1(x) + 3bg_1(x) + abf_1(x)g_1(x) = 1$
Once again, we have the same two cases and the same conditions so that all the none constant terms fall out.

Therefore $(\mathbb{Z}/4\mathbb{Z})^{\times} = \{(1+4\mathbb{Z})+(2+4\mathbb{Z})f(x), (3+4\mathbb{Z})+(2+4\mathbb{Z})f(x) \mid f(x) \in (\mathbb{Z}/4\mathbb{Z})[x]$.

2). Show that $(2, x)$ is a non-principal, prime ideal in $\mathbb{Z}[x]$.

$(2, x) = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$

First, let's make sure that this is a prime ideal. Assume:

$$\alpha\beta = xf(x) + 2g(x)$$

and AWLOG that $\alpha \notin (2, x)$. Thus $\beta \mid xf(x)$ and $\beta \mid 2g(x)$. Note that if $b = 2$ or $b = x$ then $b \in (2, x)$, so AWLOG that $b \neq x$ and $b \neq 2$. Then $b \mid f(x)$ and $b \mid g(x)$. But then $\alpha = xh(x) + 2i(x)$ for some $h(x), i(x) \in \mathbb{Z}[x]$ and thus $\alpha \in (2, x)$, a contradiction.

Therefore, $(2, x)$ is prime.

Now show that it is not principal. ABC that $(2, x) = (h(x))$ where $h(x) \in (2, x)$.
Note that $(2, x)$ is a proper ideal in $\mathbb{Z}[x]$, since the coefficient of all constant terms in $(2, x)$ must be even.
Since $2 \in (2, x)$, there must exist $g(x) \in \mathbb{Z}[x]$ such that $h(x)g(x) = 2$ and thus,
$\deg(2) = \deg((h(x)g(x)) = \deg(g(x)) + \deg(g(x)) = 0$, and so, $\deg(h(x)) = \deg(g(x)) = 0$ and thus $h(x)$ is constant.
But since 2 is prime, the only candidates are $h(x) = \{\pm 1, \pm 2\}$.
But ± 1 are units and their inclusion in the ideal would make it non-proper, so only ± 2 are left.
But $x \in (2, x)$ as well, so there must exist $f(x) \in \mathbb{Z}[x]$ such that $x = \pm 2f(x)$. But this can only happen when $f(x) = \pm\frac{x}{2}$, resulting in non-integer coefficients. a contradiction.

Therefore, $(2, x)$ is not principal.

3). Show that $F[x, y]$ is not a PID.

It was proven in class that in order for an ideal I to be a PID, then $\forall\, a, b \in I$, a and b must have a non-unit GCD in I.

Consider (x, y), an ideal in $F[x, y]$. Note that this ideal is proper, since it does not contain any non-zero constant terms.
$x \in (x, y)$ and $y \in (x, y)$ but both x and y are prime in $F[x, y]$ and thus have no common divisor other than 1. So (x, y) is not principle.

Therefore $F[x, y]$ is not a PID.

4). Prove that $R_{-2}^{\times} = \{\pm 1\}$

Assume $\alpha \in R_{-2}$
Let $\alpha = a + b\sqrt{-2}$ where $a, b \in \mathbb{Z}$
By the unit criterion, in order for α to be a unit in R_{-2}:

$$N(\alpha) = a^2 + 2b = 1$$

Note that any value of $b > 0$ is too big, and so $b = 0$, and so:
$a^2 = 1$
$a = \pm 1$

$\therefore R_{-2}^{\times} = \{\pm 1\}$

5). Let d be a squarefree integer other than 1. Show that:

$$d \equiv 2 \text{ or } 3 \pmod 4 \implies R_d = \mathbb{Z}[\sqrt{d}]$$

Assume $d \equiv 2$ or $3 \pmod 4$

$\implies$ Assume $\alpha \in R_d$

Let $\alpha = r + \sqrt{d}$

By the integer criterion:

$$N(\alpha) = r^2 - ds^2 \in \mathbb{Z}$$

$$T(\alpha) = 2r \in \mathbb{Z}$$

Then:

$$-4N(\alpha) + T(\alpha)^2 = 4(ds^2 - r^2) + (2r)^2 = 4ds^2 = d(2s)^2 \in \mathbb{Z}$$

Since $s \in \mathbb{Q}$, let $2s = \frac{a}{c}$ where $(a, c) = 1$ and $c \neq 0$
Let $d\left(\frac{a}{c}\right)^2 = k \in \mathbb{Z}$
$da^2 = kc^2$
Now, ABC that there exists prime p such that $p \mid c$
$p^2 \mid c^2$
But $(a, c) = 1$, so $p^2 \nmid a^2$, and thus $p^2 \mid d$
CONTRADICTION! Since d is squarefree
Thus, $c = 1$ and $d\left(\frac{a}{c}\right)^2 = d(2s)^2 \in \mathbb{Z}$
And since $d \in \mathbb{Z}$, we have $2s \in \mathbb{Z}$

Now, let $a = 2s \in \mathbb{Z}$ amd $b = 2r \in \mathbb{Z}$
$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{d}$
$N(\alpha) = \left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = \frac{a^2 - db^2}{4}$
$a^2 - db^2 = 4N(\alpha) \equiv 0 \pmod 4$
and so: $a^2 \equiv db^2 \pmod 4$

Now, consider the even/odd cases for a and b
Recall: $\forall\, n \in \mathbb{Z}, n$ is even $\iff n^2$
Assume $n \in \mathbb{Z}$:

Case 1: $n \,\text{even}$

Case 1a: $n \equiv 0 \pmod 4$

$$n^2 \equiv 0 \cdot 0 \pmod 4 \equiv 0 \pmod 4$$

Case 1b: $n \equiv 2 \pmod 4$

$$n^2 \equiv 2 \cdot 2 \pmod 4 \equiv 0 \pmod 4$$

Thus, $n \,\text{even} \implies n^2 \equiv 0 \pmod 4$

Case 2: $n \,\text{odd}$

Case 2a: $n \equiv 1 \pmod 4$

$$n^2 \equiv 1 \cdot 1 \pmod 4 \equiv 1 \pmod 4$$

Case 2b: $n \equiv 3 \pmod 4$

$$n^2 \equiv (-1) \cdot (-1) \pmod 4 \equiv 1 \pmod 4$$

Thus, $n \,\text{odd} \implies n^2 \equiv 1 \pmod 4$

Now, apply this information to a and b based on d:

Case 1: $d \equiv 2 \pmod 4$

$a^2 \equiv 2b^2 \pmod 4$
and so $a^2, b^2 \equiv 0 \pmod 4$, and thus a and b must both be even
Thus $r = \frac{a}{2}$ and $s = \frac{b}{2}$ are both integers

$\therefore \alpha \in \mathbb{Z}[\sqrt{d}]$

Case 2: $d \equiv 3 \pmod 4$

$a^2 \equiv -b^2 \pmod 4$
and so $a^2, b^2 \equiv 0 \pmod 4$, and thus a and b must both be even and this is the same as the previous case

$\therefore \alpha \in \mathbb{Z}[\sqrt{d}]$

$\Longleftarrow$ Assume $\alpha \in \mathbb{Z}[\sqrt{d}]$

Let $\alpha = m + n\sqrt{d}$ where $m, n \in \mathbb{Z}$

$N(\alpha) = m^2 - dn^2 \in \mathbb{Z}$

$T(\alpha) = 2m \in \mathbb{Z}$

Therefore, by the integer criterion, $\alpha \in R_d$

$\therefore R_d = \mathbb{Z}[\sqrt{d}]$

6). Show that R_{-13} is not a UFD.

Since $(-13) \equiv 3 \pmod 4$, $R_{-13} = \mathbb{Z}[\sqrt{-13}]$.
Also, since $13 > 4$, $\mathbb{Z}[\sqrt{-13}]^\times = \{\pm 1\}$.

Consider $14 \in \mathbb{Z}[\sqrt{-13}]$
$2 \cdot 7 = 14$ and $(1 + \sqrt{-13})(1 - \sqrt{-13}) = 14$

$2(1 + \sqrt{-13}) \neq \pm 1$
$2(1 - \sqrt{-13}) \neq \pm 1$
$7(1 + \sqrt{-13}) \neq \pm 1$
$7(1 - \sqrt{-13}) \neq \pm 1$

Thus, none of the factors are associates.

ABC: 2 is not irreducible in $\mathbb{Z}[\sqrt{-13}]$
$\exists\, \alpha, \beta \in \mathbb{Z}[\sqrt{-13}], \alpha\beta = 2$
$N(2) = N(\alpha)N(\beta) = 4$
We can discount $4 \cdot 1$ because a norm of 1 indicates a unit and thus the factorization differs only by a unit.
Thus $N(\alpha) = N(\beta) = 2$
But $x^2 + 13y^2 = 2$ has no integer solutions. CONTRADICTION!

Therefore 2 is irreducible in $\mathbb{Z}[\sqrt{-13}]$

ABC: 7 is not irreducible in $\mathbb{Z}[\sqrt{-13}]$
$\exists\, \alpha, \beta \in \mathbb{Z}[\sqrt{-13}], \alpha\beta = 7$
$N(7) = N(\alpha)N(\beta) = 49$
We can discount $49 \cdot 1$ because a norm of 1 indicates a unit and thus the factorization differs only by a unit.
Thus $N(\alpha) = N(\beta) = 7$
But $x^2 + 13y^2 = 7$ has no integer solutions. CONTRADICTION!

Therefore 7 is irreducible in $\mathbb{Z}[\sqrt{-13}]$

ABC: $1 \pm \sqrt{-13}$ is not irreducible in $\mathbb{Z}[\sqrt{-13}]$
$\exists\, \alpha, \beta \in \mathbb{Z}[\sqrt{-13}], \alpha\beta = 1 \pm \sqrt{-13}$
$N(1 \pm \sqrt{-13}) = N(\alpha)N(\beta) = 14$
We can discount $14 \cdot 1$ because a norm of 1 indicates a unit and thus the factorization differs only by a unit.
Thus, WLOG: $N(\alpha) = 2$ and $N(\beta) = 7$
But we have already proven that no such α or β exist in $\mathbb{Z}[\sqrt{-13}]$.
CONTRADICTION!

Therefore $1 \pm \sqrt{-13}$ is irreducible in $\mathbb{Z}[\sqrt{-13}]$

So, there exists two distinct factorization of 14 into irreducibles that are not associates.

Therefore R_{-13} is not a UFD.