School of Mathematical and Computational Sciences
Abstract Algebra

Prof. Pablo Rosero
& Christian Chávez
Problem Set 6

EDs, PIDs, UFDs, and Polynomial Rings

(Lessons 12, 13 and 14)

1. Let R be an integral domain. Prove that if two elements d and d' of R generate the same principal ideal, i.e., $\langle d\rangle = \langle d'\rangle$, then $d' = ud$ for some $u \in R^{\times}$. Conclude that if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some $u \in R^{\times}$.

2. Consider the ring

$$R = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] = \left\{ m + n\frac{1+\sqrt{-d}}{2} \mid m, n \in \mathbb{Z}\right\}$$
$$= \left\{ \frac{a+b\sqrt{-d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}$$

where d is square-free and $d \equiv 3 \pmod 4$. Let $N(r) = r\bar{r}$, where $\bar{r}$ is the conjugate of r.

(i) Suppose that for any complex number z, there exists $\xi \in R$ such that $N(z-\xi) < 1$. Show that N is a Euclidean function on R. Conclude that R is a Euclidean domain.

(ii) Show that $R = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a Euclidean domain.

3. Prove that every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

4. Prove that any two nonzero elements of a P.I.D. have a least common multiple.

5. Let R be an integral domain and suppose that every prime ideal in R is principal. Prove that every ideal of R is principal. i.e., R is a P.I.D.

6. Show that the ideal $I = \langle 3, x^3 - x^2 + 2x - 1\rangle$ in $\mathbb{Z}[x]$ is not principal.

7. Find the greatest common divisor (GCD) of the polynomials $g = x^3 + x^2 + x - 3$ and $f = x^4 - x^3 + 3x^2 + x - 4$ in $\mathbb{Q}[x]$ using the Euclidean algorithm.

8. Let $R = \mathbb{Z}[\sqrt{-5}]$.

(i) Prove that 2, $\sqrt{-5}$, and $1+\sqrt{-5}$ are irreducible in R.

(ii) Prove that R is not a unique factorization domain (UFD).

(iii) Provide an explicit ideal in R that is not principal.

9. Show that the polynomial

$$(x-1)(x-2)\cdots(x-n) - 1$$

is irreducible over $\mathbb{Z}$ for all $n \geq 1$.

10. Show that the polynomial

$$(x-1)(x-2)(x-n)+11$$

is irreducible over $\mathbb{Z}$ for all $n \geq 1$, $n \neq 4$.

11. Let $A[[x]]$ denote the set of sequences $(a_i)_{i\in\mathbb{Z}^+}$ of elements of A, without any restriction. Define the addition and multiplication of two elements $(a_i)_{i\in\mathbb{Z}^+}$ and $(b_i)_{i\in\mathbb{Z}^+}$ of $A[[x]]$ as follows:

$$(a_i)_{i\in\mathbb{Z}^+} + (b_i)_{i\in\mathbb{Z}^+} = (a_i + b_i)_{i\in\mathbb{Z}^+}$$

and

$$(a_i)_{i\in\mathbb{Z}^+}(b_i)_{i\in\mathbb{Z}^+} = (c_k)_{k\in\mathbb{Z}^+},$$

where $c_k = \sum_{i+j=k} a_i b_j$. Show that these operations make $A[[x]]$ a commutative ring and that $A[x]$ is a subring of $A[[x]]$. The ring $A[[x]]$ is called the *ring of formal power series* in x: this name comes from the fact that, if we set $x = (0,1,0,\dots) \in A[[x]]$, then every element $(a_i)_{i\in\mathbb{Z}^+}$ of $A[[x]]$ can be formally written as:

$$\sum_{i=0}^{\infty} a_i x^i.$$

12. Prove that $x^3 + nx + 2$ is irreducible in $\mathbb{Z}[x]$ for all integers $n \neq 1, -3, -5$.

13. Determine whether the following polynomials are irreducible in the rings indicated. For those that are irreducible, determine their factorization into irreducibles.

(i) $x^3 + x + 1$ in $\mathbb{Z}_3[x]$.

(ii) $x^5 + 1$ in $\mathbb{Z}_5[x]$.

(iii) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

14. Apply Eisenstein's criterion to establish the irreducibility of each of the following polynomials over $\mathbb{Q}$:

(i) $x^3 + 6x^2 + 2x + 2$,

(ii) $x^5 - 2x^3 + 10$,

(iii) $x^4 + 6$,

(iv) $x^7 - 31$,

(v) $2x^4 - 27x^3 + 6x^2 - 9x + 6$,

(vi) $x^3 + 5x^2 + 25x + 5$.

15. Let A be a ring. Prove that

$$\frac{A[x,y]}{\langle x-y\rangle} \cong A[x] \cong A[y].$$