8.1 Euclidean Domains

3) Let R be a Euclidean domain with norm n, and m the minimum over the norm of all nonzero elements of R. If $n(a) = m$ for some nonzero $a \in R$, then a is a unit.

Proof: R is a Euclidean domain, and so there exist unique $q, r \in R$ where $1 = qa + r$ and where $r = 0$ or $n(r) < n(q)$. If $r = 0$, we are finished, so assume $r \neq 0$, then $n(r) < n(q)$. We also have that $1 = aq + r$ since R is commutative, thus $n(r) < n(a)$. This is a contradiction however, since by assumption $n(a)$ is minimal over nonzero elements of R. This shows that $r = 0$, completing the proof. ■

8.2 Principal Ideal Domains

3) If R is a principal ideal domain and P a prime ideal of R, then R/P is also a principal ideal domain.

Proof: If $P = (0)$, then $R/P \cong R$ and we are done. Otherwise, P is nonzero. Since every non-zero prime ideal in a principal ideal domain is maximal, we have that R/P is a field, and thus a principal ideal domain. ■

9.2 Polynomial Rings over Fields

1) Given a field F, fix $f \in F[X]$ with degree $n \geq 1$. Additionally, fix $g \in F[X]$, and denote $\bar{g} = g + (f) \in F[X]/(f)$, then there exists a unique polynomial $r \in F[X]$ with degree strictly less than n where $\bar{g} = \bar{r}$.

Proof: Since $F[X]$ is a Euclidean domain with the norm being the degree of the polynomial, there exist unique polynomials $q, r \in F[X]$ where $g = qf + r$, and where $r = 0$ or $\deg r < \deg q$. This shows that $g \in \bar{r}$, but this also implies that $r = g + (-q)f$, thus $r \in \bar{g}$ and $\bar{g} = \bar{r}$, proving the existence of such an r. By the division algorithm r is unique, thus we are finished. ■

2) Let F be a finite field of order q and fix $f \in F[X]$ with degree $n \geq 1$, then we have that $|F[X]/(f)| = q^n$.

Proof: We established that the elements in $|F[X]/f(x)|$ are in bijection with the polynomials in $F[X]$ of degree strictly less than n, i.e. the polynomials $g \in F[X]$ that take the form

$$g(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

for elements $a_i \in F$. Since we have n coefficients and q options for each coefficient, it is clear that there are q^n polynomials of this form. ■

3) For a field F and polynomial $f \in F[X]$, we have that $F[X]/(f)$ is a field if and only if f is irreducible.

Proof: First assume $F[X]/(f)$ is a field. This is equivalent to (f) being a maximal ideal in $F[X]$, but since $F[X]$ is a principal ideal domain, we have that (f) is prime, and in turn f is prime, and thus irreducible in $F[X]$.

Conversely, assume f is irreducible. Again, because $F[X]$ is a P.I.D., f is prime, thus the ideal (f) of $F[X]$ is prime and thus maximal, showing that $F[X]/(f)$ is a field. ■

9.3 Polynomial Rings that are Unique Factorization Domains

3) Fix a field F and denote R as the set of polynomials $f \in F[X]$ that take the form

$$f(X) = a_0 + a_2X^2 + \cdots + a_nX^n$$

with elements $a_i \in F$. Then R is a ring, but not a unique factorization domain.

Proof: Consider the polynomials X^2 and X^3 in R. Since $X \notin R$, and since 2 and 3 are prime, we have that X^2 and X^3 are irreducible. Additionally, X^2 and X^3 are clearly not associates. We can see that

$$X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3,$$

thus we have obtained two factorizations of X^6 with non-associate irreducible factors, thus showing that R is not a U.F.D. ■

9.4 Irreducibility Criteria

1) For $p \in \mathbb{F}_2[X]$ defined as $p(X) = X^2 + X + 1$, we have that

$$p(0) = 0^2 + 0 + 1 = 1^2 + 1 + 1 = 1,$$

showing that p has no root in $\mathbb{F}_2$, and thus is irreducible.

If we define $p \in \mathbb{F}_3[X]$ as $p(X) = X^3 + X + 1$, then

$$p(\bar{1}) = \bar{1}^3 + \bar{1} + \bar{1} = \bar{0},$$

thus it has a root in $\mathbb{F}_3$ and is reducible.

Next, define $p \in \mathbb{F}_5[X]$ as $p(X) = X^4 + 1$, then if $p(X-1)$ is irreducible, then so is $p(X)$. We evaluate $p(X-1)$ as

$$p(X-1) = (X-1)^4 + 1 = X^4 - 4X^3 + 6X^2 - 4X^2 + 2,$$

and note that $2 \mid -4$, $2 \mid 6$, $2 \mid -4$, and $2 \mid 2$, but $2^2 \mid 2$, thus p is irreducible.

2) In $\mathbb{Z}[X]$, we have that $X^4 - 4X^3 + 6$ is irreducible by Eisenstein's criterion, since $2 \mid -4$ and $2 \mid 6$, but $2^2 \nmid 6$. Similary for $X^6 + 30X^5 - 15X^3 + 6X - 120$, we have that $3 \mid 30$, $3 \mid -15$,$3 \mid 6$, and $3 \mid 120$, but $3^3 \nmid 120$, thus it is irreducible. Finally, consider $p(X) = X^4 + 4X^3 + 6X^2 + 2X + 1$. It is clear that if $p(X-1)$ is irreducible, then so is $p(X)$. Evaluating $p(X-1)$, we have that

$$p(X-1) = x^4 - 8x^3 - 2x + 2.$$

Since $2 \mid -8$, $2 \mid -2$, and $2 \mid 2$, but $2^2 \nmid 2$, we have by E.C. that p is irreducible.

5) A monic polynomial in $\mathbb{F}_2[X]$ has no root when the constant coefficient is $\bar{1}$ and the number of nonzero coefficients is odd. Thus, the irreducible monic polynomials of $\mathbb{F}_2[X]$ with degree at most 3 are given by $X^3 + X + 1$ and $X^3 + X^2 + 1$.

6) Define the polynomial $p \in \mathbb{F}_3[X]$ as $p(X) = X^2 + 1$. It is clear that p has no root in $\mathbb{F}_3$, and thus it is irreducible. Since $\mathbb{F}_3[X]$ is a principal ideal domain, we have that p is prime, thus the ideal (p) is prime and thus maximal. This implies that $\mathbb{F}_3[X]/(X^2+1)$ is a field. Additionally, we established that this field has order $3^2 = 9$, and thus we have constructed a field of order 9.