Notes on Rings and Polynomials: The purpose of these notes is to give a businesslike account of what you need to know from ring theory for this class.

Let $\boldsymbol{F}$ be a field. A *polynomial* in $\boldsymbol{F}$ is an expression of the form

$$P(x) = a_0 + a_1 x + ... + a_n x^n, \qquad a_0, ..., a_n \in \boldsymbol{F}.$$

Assuming a_n is nonzero, the *degree* of P is n, We denote this by writing $\deg(P) = n$. The set of all polynomials is a ring with respect to the usual addition and multiplication. It is denoted $\boldsymbol{F}[x]$. There are 4 basic facts we want to know:

1. $\boldsymbol{F}[x]$ is a Euclidean domain.
2. $\boldsymbol{F}[x]$ is a Principle Ideal Domain.
3. If P is an irreducible polynomial then $\boldsymbol{F}[x]/(P)$ is a field.
4. $\boldsymbol{F}[x]$ is a Unique Factorization Domain.

I'll prove these statements in turn, and give relevant definitions as I go.

Euclidean Domain: We begin with a preliminary lemma.

Lemma 0.1 *If P and Q are polynomials with $\deg(Q) \geq \deg(P)$ then we can find some polynomial D_1 such that $\deg(Q - D_1 P) < \deg(Q)$.*

Proof: Let $K = \deg(Q) - \deg(P)$. Write

$$P = a_0 + ... + a_n x^n, \qquad Q = b_0 + ... + b_{n+K} x^{n+K},$$

with $a_n \neq 0$. Let $D_1 = (b_{n+K}/a_n) x^K$. We compute that

$$Q - D_1 P = b_0 + ... + b_{n+K-1} x^{n+K-1}.$$

Hence $\deg(Q - D_1 P) \leq n + K - 1 < \deg(Q)$. ♠

Theorem 0.2 $\boldsymbol{F}[x]$ *is a Euclidean Domain. In other words, given any polnomials P and Q then there is some polynomial D such that $Q = DP + R$ where either $R = 0$ or $\deg(R) < \deg(P)$.*

Proof: If $\deg(Q) < \deg(P)$ we can take $D = 0$ and $R = Q$. Now assume that $\deg(Q) \geq \deg(P)$. The proof goes by induction on $\deg(Q) - \deg(P)$. By Lemma 0.1 we can find some polynomial D_1 such that $\deg(Q - D_1P) < \deg(Q)$. Let $Q_1 = Q - D_1P$. Since $\deg(Q_1) < \deg(Q)$ we can use the induction step to find some polynomial D_2 such that $Q_1 = D_2P + R$ with either $R = 0$ or $\deg(R) < \deg(P)$. But then we have

$$Q = Q_1 + D_1P = (D_2P + R) + D_1P = (D_1 + D_2)P + R.$$

Setting $D = D_1 + D_2$ we have $Q = DP + R$, as desired. ♠

Principle Ideal Domain: An *ideal* in $\boldsymbol{F}[x]$ is any sub-ring $I \subset \boldsymbol{F}[x]$ such that $PI \subset I$ for all $r \in \boldsymbol{F}[x]$. Here $PI = \{PQ | \ Q \in I\}$. I is called *principle* if there is a single element $P \in \boldsymbol{F}[x]$ such that $I = P\boldsymbol{F}[x]$. In other words, every element of I is a multiple of P. We will write $I = (P)$ in this case.

Theorem 0.3 *$\boldsymbol{F}[x]$ is a PID: Every ideal is principle.*

Proof: Choose some $P \in I$ which has smallest degree. We want to show that every other $Q \in I$ is a multiple of P. Suppose not. Since $\boldsymbol{F}[x]$ is a Euclidean Domain, we can write $Q = DP + R$ where $\deg(R) < \deg(P)$ and R is nonzero. (Otherwise Q is a multiple of P.) Note that $R = Q - DP \in I$ because I is an ideal. This contradicts the fact that P is the member of I with smallest degree. ♠

Maximal Ideals: In the definitions to follow, we insist that the polynomial P is not a constant polynomial. That is, $\deg(P) \geq 1$. The polynomial P is *reducible* if $P = AB$ where A and B are two polynomials such that $\deg(A) < \deg(P)$ and $\deg(B) < \deg(P)$. If P is not reducible, it is called *irreducible*. When polynomials P and A are multiples of each other, they are called *associate*.

Lemma 0.4 *If P is irreducible and a multiple of some polynomial A, then A is either constant or an associate of P.*

Proof: If $P = AB$ then $\deg(P) = \deg(A) + \deg(B)$. When P is irreducible, we have $\deg(A) = 0$ or $\deg(B) = 0$. In the first case A is a constant and in the second case A is an associate of P. ♠

An ideal $I \subset \boldsymbol{F}[x]$ is *maximal* if there is no other ideal J such that $I \subset J$ and $J \neq I$ and $J \neq \boldsymbol{F}[x]$.

Lemma 0.5 *If P is irreducible, then the ideal (P) is maximal.*

Proof: Let $I = (P)$. If I is not maximal, then we can find the above kind of J. Since $\boldsymbol{F}[x]$ is a PID, all elements of I, including P, are multiples of some $S \in J$. But since P is irreducible either P and S are associates or else S is a constant. In the first case $I = J$ and in the second case $J = \boldsymbol{F}[x]$. This contradiction shows that I is maximal. ♠

Lemma 0.6 *Suppose that R is a commutative ring with* 1 *which has no ideals other than the trivial ideal and R. Then R is a field.*

Proof: Let $a \in R$ be arbitrary nonzero element. Consider the ideal (a) consisting of all multiples of R. Since (a) contains $1a = a$, it is nontrivial. Hence $(a) = R$. But then $1 \in (a)$. So, there is some $b \in \boldsymbol{R}$ such that $ab = 1$. This shows that $R - \{0\}$ is an abelian group. Hence R is a field. ♠

Now for the main result.

Theorem 0.7 *If P is irreducible, then the quotient ring $\boldsymbol{F}[x]/(P)$ is a field.*

Proof: Recall that $R = \boldsymbol{F}[x]/(P)$ consists of the cosets of P, namely elements of the form $a + (P)$ where a is some polynomial. The addition and multiplication laws are given by

$$[a_1+(P)]+[a_2+(P)] = [(a_1+a_2)+(P)], \qquad [a_1+(P)][a_2+(P)] = [(a_1a_2)+(P)].$$

The element $1 + (P)$ serves as "the 1" in R, so R is a commutative ring with 1. Suppose, for the sake of constraciction, that R is not a field. Then R has some nontrivial proper ideal J. Let $I \subset R$ consists of all those cosets $a + (P)$ with $a \in J$. The addition and multiplication laws guarantee that I is an ideal of R. Note that $(P) \subset I$. Since (P) is maximal, $I = R$. But then $1 + (P) \in J$. Since J contains "the 1", we must have $J = R$. This is a contradiction. Hence R is a field. ♠

Unique Factorization Domain: Now we show that $\boldsymbol{F}[x]$ is a unique factorization domain.

Lemma 0.8 *Every polynomial in $\boldsymbol{F}[x]$ factors into irreducibles.*

Proof: Let P be such a polynomial. The proof goes by induction on $\deg(P)$. If $\deg(P) \leq 1$ the result is true because there are no two positive integers whose sum is at most 1. In general, if P is reducible, we can write $P = AB$ where $\deg(A) < \deg(P)$ and $\deg(B) < \deg(P)$. But then, by induction, A and B factor into irreducibles. Multiply these together and you get a factoring of P into irreducibles. ♠

To show that $\boldsymbol{F}[x]$ is a UFD, we want to show that the factorization above is unique. We need a few preliminary lemmas first.

Lemma 0.9 *Suppose that P is irreducible and Q is any other polynomial. Then either Q is a multiple of P or there are polynomials M and N such that $PM + QN = 1$.*

Proof: Let I be the set of polynomials of the form $PM + QN$. By construction I is an ideal. Let S be some element of I having minimal degree. We already know that every element of I is a multiple of S. Since $P \in I$, we know that P is a multiple of S. Since P is irreducible, either S is a constant or P is a multiple of S.

If S is a constant, then the equation $S = MP + NQ$ gives

$$1 = (M/S)P + (M/S)Q.$$

This works because $\boldsymbol{F}$ is a field. The other possibility is that $S = cP$ for some constant c. But then, since $Q \in I$, we know that Q is a multiple of cP. That is, $Q = D(cP)$. But then $Q = (cD)P$. Hence Q is a multiple of P. ♠

Lemma 0.10 *If P is irreducible and AB is a multiple of P then either A is a multiple of P or B is a multiple of P.*

Proof: If this is false, then by the previous lemma we have

$$1 = M_1P + N_1A, \qquad 1 = M_2P + N_2A.$$

Multiply these together and collect terms, to give

$$1 = M_3P + N_3(AB).$$

Since $AB = DP$ we can write

$$1 = M_3P + N_3(DP) = M_4P.$$

But then $0 = \deg(M_4) + \deg(P)$, which is a contradiction. ♠

Lemma 0.11 *Suppose that A is irreducible and $B_1, ..., B_n$ are irreducible. If $B_1...B_n$ is a multiple of A then some B_j is an associate of A.*

Proof: By the preceding lemma, either B_1 is a multiple of A or else $B_2...B_n$ is a multiple of A. Repeating this argument, either B_2 is a multiple of A or else $B_3...B_n$ is a multiple of A. In this way we must reach some index j such that B_j is a multiple of A. But then B_j and A are associates. ♠

Theorem 0.12 *$\boldsymbol{F}[x]$ is a UFD. That is, every polynomial factors uniquely into irreducibles, up to reording the factors or replacing some of the factors by associates.*

Proof: We already have shown that any polynomial factors into irreducibles. We just have to take care of uniqueness. Suppose that

$$P = A_1...A_m = B_1...B_n$$

with all the factors irreducible. If the uniqueness fails, we can take a counter-example where m is as small as possible. For this minimal example, none of the As is an associate of any of the Bs because otherwise we could cancel off associates from both sides and get a smaller counter-example. However, since $B_1...B_n$ is a multiple of A_1, the previous lemma says that B_j is an associate of A_1 for some j. This is a contradiction. ♠