We will first summarise the general results that we will need from the theory of rings. A UNITAL RING, R, is a set equipped with two binary operations $+$ and $\cdot$ such that $(R, +)$ is an abelian group and, for all $r, s, t \in R$, the following axioms hold.

(R1) There is an element $1 \in R$ such that $1 \cdot r = r \cdot 1 = r$ (the UNIT ELEMENT).

(R2) $r \cdot s \in R$.

(R3) $r \cdot (s \cdot t) = (r \cdot s) \cdot t$, the ASSOCIATIVITY axiom.

(R4) $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(r + s) \cdot t = r \cdot t + s \cdot t$, the DISTRIBUTIVITY axioms.

For $r \cdot s$ we will write simply rs. Note that it is not required that an element $r \in R$ has a multiplicative inverse but, if it does, we call it a UNIT of R. We assume some basic familiarity with rings and move immediately to summarise some of the special classes of rings in which we will be interested. A ring R is

1. a COMMUTATIVE RING if $rs = sr$ for all $r, s \in R$.
2. an INTEGRAL DOMAIN if is commutative and contains no zero divisors (recall a ZERO DIVISOR of a commutative ring R is an element $0 \neq r \in R$ such that $rs = 0$ for some $0 \neq s \in R$);
3. a DIVISION RING if its nonzero elements are all units (i.e. they form a group under multiplication);
4. a FIELD if it is a commutative division ring.

For the remainder of the course, "ring" will mean "commutative unital ring".

It is not our purpose here to conduct an extensive study of rings in general. We now introduce the classes of rings which will interest us most throughout the course.

The Integers: Everybody's favourite ring! Well, OK, this may be a slight exaggeration, but it is the properties of $\mathbb{Z}$ that will most influence the direction the course takes for quite a while. The ring $\mathbb{Z}$ is an integral domain but not a field. The elements ± 1 are the only units of $\mathbb{Z}$.

Polynomial rings: Suppose that R is any ring. Then the set $R[x]$ of all polynomials in the indeterminate x having coefficients in the ring R is also a ring, called a POLYNOMIAL RING (over R in

1 indeterminate). Notice that $R[x]$ is commutative, and that $R[x]$ is an integral domain if and only if R is. For an element $f(x) \in R[x]$, define the DEGREE of f(x), denoted $\deg(f)$, to be the highest power of x occurring in $f(x)$ (with nonzero coefficient). The units of $R[x]$ are the scalar polynomials $f(x) = r$, where r is a unit of R. We will be especially interested in polynomial rings in the special case when $R = \mathbb{F}$ is a field.

Matrix rings: Once again, suppose that R is any ring, and let n be a positive integer. Then the set $\mathbb{M}_n(R)$ of all $n \times n$ matrices whose entries are elements of R is also a ring. Unlike polynomial rings, not many of the nice properties of R are preserved when one moves to a matrix ring over R. Note that $M_n(R)$ is commutative iff $n = 1$. Also, if R is an integral domain, then $M_n(R)$ is an integral domain iff $n = 1$. Take the case $n = 2$, $R = \mathbb{R}$ for example; then $r = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is a zero divisor, since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Again the special case when $R = \mathbb{F}$ is a field will be of greatest interest to us. Note that, in this case, the set of units of $M_n(\mathbb{F})$ is the set (actually, group) of all invertible matrices; we denote this set by $GL_n(\mathbb{F})$.

We next introduce some structural notions concerning rings. A SUBRING S of a ring R is a subset of R which is also a ring. In general, if $S \subset R$ is a subring and $r \in R$, then $rS \not\subseteq S$ (i.e. S is not stable under multiplication by R). Subrings which do have this property play a central role in ring theory, completely analogous to that played by normal subgroups in group theory. A subring $I \subset R$ is an IDEAL of R, denoted $I \leq R$, if, for all $r \in R$ and $a \in I$ we have $ra \in I$. An ideal $I \leq R$ is PROPER if $0 < I < R$. An ideal $I < R$ is: MAXIMAL if it is not properly contained in any other ideal; and PRIME if whenever $J_1 J_2 \subset I$ for ideals J_1, J_2 of R, either $J_1 \subset I$ or $J_2 \subset I$. It turns out that the collection of prime ideals of a ring properly contains the collection of maximal ideals (see Exercise 3).

Recall that, if N is a normal subgroup of G, then we can form the factor group G/N consisting of "cosets" $\{gN \mid g \in G\}$ under the operation $(gN)(hN) = ghN$. We can do exactly the same if $I \leq R$ is an ideal. The FACTOR RING R/I is the set $\{r + I \mid r \in R\}$ with operations $(r+I)+(s+I) = (r+s)+I$ and $(r + I) \cdot (s + I) = rs + I$ (see Exercise 1).

A map $\varphi \colon R \to S$ between rings R and S is a RING HOMOMORPHISM if it preserves the ring structure, namely for all $r, s \in R$ $\varphi(r + s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$. If $\varphi \colon R \to S$ is ring homomorphism then $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$ is an ideal of R and $\operatorname{im}\varphi = \{\varphi(r) \mid r \in R\}$ is a subring of S (see Exercise 2); φ is an EPIMORPHISM if $\operatorname{im}\varphi = S$; φ is a MONOMORPHISM if $\ker\varphi = 0$; and φ is a ISOMORPHISM if it is both a monomorphism and an epimorphism.

Note that, if I is an ideal of R, then there is a (canonical) epimorphism $\pi \colon R \to R/I$ sending $r \mapsto r + I$ and $\ker\pi = I$. Hence we have the following 1-1 correspondence:

$$\boxed{\{ \text{ ideals of } R \} \longleftrightarrow \{ \text{ kernels of ring homomorphisms } R \to S \}}$$

We next introduce an important class of rings. If $a \in R$, then the set $Ra = \{ra \mid r \in R\}$ is an ideal of R called a PRINCIPAL IDEAL of R and denoted (a) (see Exercise 5). Note that $(a) = R$ iff a is a unit of R. A ring R is called a PRINCIPAL IDEAL RING if all of its ideals are principal. A principal ideal ring which is also an integral domain is called a PRINCIPAL IDEAL DOMAIN, or PID and will be of particular interest to us in what follows. The prototypical example of a PID is the ring of integers $\mathbb{Z}$. We now wish to show that $\mathbb{F}[x]$ is a PID. This will not prove too difficult and uses only facts that we have "known" about polynomials for as long as we can remember. The same arguments hold inside $\mathbb{Z}$ so, if it is not already clear why $\mathbb{Z}$ is a PID, then it should soon be.

(Rgs1) Lemma [Division Algorithm]. *Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x]$. Then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$.*

Proof. Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ and $g(x) = b_m x^m + \ldots + b_1 + b_0$. We proceed by induction on $\deg(f)$ to show the existence of $q(x)$ and $r(x)$. The result is trivial if $\deg(f) \leq \deg(g)$ so we may assume that $\deg(f) > \deg(g)$. Set $f_0(x) := f(x) - (a_n/b_m)x^{n-m}g(x)$ and note that $\deg(f_0) < \deg(f)$. By induction, there exist $q_0(x), r_0(x) \in \mathbb{F}[x]$ with $\deg(r_0) < \deg(g)$ such that $f_0(x) = q_0(x)g(x) + r_0(x)$. Setting $q(x) := q_0(x) + (a_n/b_m)x^{n-m}$ and $r(x) := r_0(x)$ does the job.

For uniqueness, suppose that $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{F}[x]$ with $\deg(r_1) \leq \deg(r_2) < \deg(g)$ are such that $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$. Then $(q_1(x) - q_2(x))g(x) = r_1(x) - r_2(x)$ so that $\deg(q_1 - q_2) + \deg(g) = \deg(r_1 - r_2) < \deg(g)$. This is impossible unless $q_1(x) = q_2(x)$ whence also $r_1(x) = r_2(x)$. $\square$

(Rgs2) Theorem. *If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a PID.*

Proof. Let $I \neq 0$ be an ideal of $\mathbb{F}[x]$, $0 \neq g(x) \in I$ have least possible degree, and let $f(x) \in I$. Then, by **(Rgs1)**, there exist $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$. Thus $r(x) = f(x) - q(x)g(x) \in I$ and it follows from the minimality of $\deg(g)$ that $r(x) = 0$. That is $f(x) \in (g(x))$, so $I = (g(x))$. $\square$

We conclude this lecture by introducing an important property which is known to hold for the ring $\mathbb{Z}$, and demonstrate that holds for generally for any PID. We say that, for elements $a, b \in R$, a is a DIVISOR of b (denoted $a|b$) and b is a MULTIPLE of a if $b = ac$ for some $c \in R$. Note that $a|b$ iff $b \in Ra = (a)$ iff $(b) \leq (a)$. A nonzero, non-unit $p \in R$ is called: IRREDUCIBLE if, for all $a, b \in R$, if $p = ab$ then either a or b is a unit; or PRIME if, for all $a, b \in R$, if $p|ab$ then either $p|a$ or $p|b$. These two candidates for the "atoms" of a ring are closely related. Indeed, the two concepts coincide in our favourite rings, $\mathbb{Z}$ and $\mathbb{F}[x]$. This turns out to be the case for all PIDs (see Exercise 7). The following result should look somewhat familiar.

(Rgs3) Theorem. *Each non-unit a of a PID R has a "prime" (or "irreducible") factorisation; that is, there exist primes $p_1, \ldots, p_n \in R$ such that $a = p_1 \ldots p_n$. Moreover such a factorisation is unique up to rearrangement.*

Proof. Since R is a PID, we may use the terms "prime" and "irreducible" interchangeably. Let $B \subset R$ denote the set of all elements which do not possess a factorisation of the type specified. Suppose that $B \neq \emptyset$, and let $b \in B$. Then b factors as $b = b_1 b_2$ where neither b_1 nor b_2 is a unit. Since $a \in B$, at least one of b_1 or b_2 does not possess a prime factorisation. Therefore there are functions $f: B \to B$ and $g: B \to R$ such that $b = f(b)g(b)$ with $g(b)$ a non-unit. Hence we obtain a proper ascending chain of ideals

$$(b) \subset (f(b)) \subset (f^2(b)) \subset \ldots \subset (f^n(b)) \subset \ldots$$

Now the join of a chain of ideals is also an ideal of R (Exercise 8) and, since R is a PID, it is necessarily principal. It follows that the join of our chain is the principal ideal $(f^m(b))$ for some m. But then the chain stabilises, contradicting the assertion that it is proper. It follows that $B = \emptyset$.

Let $a = p_1 \ldots p_n = q_1 \ldots q_n$ be two prime factorisations of a with n minimal. We show uniqueness by induction on n. Since p_1 is prime, it follows that p_1 is a factor of some q_i; we may assume $p_1 | q_1$. But q_1 is also irreducible, so $p_1 = q_1 u$ for some unit $u \in R$. Thus $p_2 p_3 \ldots p_n = (uq_2) q_3 \ldots q_m$, and the proof of uniqueness now follows easily. $\square$

The operation "$|$" places a partial order on the elements of R. Using this simple observation we can now define a concept which, again, is familiar to our favourite ring $\mathbb{Z}$ (and, perhaps less so, to $\mathbb{F}[x]$). For elements $a_1, \ldots a_k$ in a PID R, define $\gcd(a_1, \ldots, a_k)$, the GREATEST COMMON DIVISOR of $a_1, \ldots, a_k$, to be the largest element $d \in R$ such that $d | a_i$ for $1 \leq i \leq k$. Similarly, $\operatorname{lcm}(a_1, \ldots, a_k)$, the LEAST COMMON MULTIPLE of $a_1, \ldots, a_k$, is the smallest element $m \in R$ such that $a_i | m$ for $1 \leq i \leq k$. Note that **(Rgs3)** guarantees the existence and uniqueness of gcds and lcms. A set $\mathcal{P}$ of a PID R is called a COMPLETE SET OF PRIMES for R if it contains exactly one generator for each of the (principle) maximal ideals of R.

Exercises.

1. If $I \leq R$, show that R/I is a ring.
2. For a ring homomorphism $\varphi: R \to S$ show that $\ker \varphi \leq R$ and that im φ is a subring of S. Is im φ always an ideal of S? Show that φ induces a ring isomorphism $R/\ker \varphi \to$ im φ.
3. (a) Show that $I < R$ is a prime ideal iff the following property holds for all $a, b \in R$: ($\clubsuit$) $ab \in I \implies$ either $a \in P$ or $b \in P$.
   (b) Show that every maximal ideal is prime.

(c) Give an example of a ring R and nonzero prime ideal I which is not maximal.

4. Show that $I < R$ is a maximal ideal iff R/I is a field.
5. For $a \in R$, show that (a) is an ideal of R.
6. Prove that a ring has precisely two ideals if and only if it is a field.
7. Let R be an integral domain. Prove each of the following:
   (a) If $p \in R$ is prime then (p) is a prime ideal.
   (b) If $p \in R$ is irreducible then (p) is a maximal principal ideal (i.e. it is not properly contained in any other *principal* ideal, but it may not be maximal).
   (c) Every prime element of R is irreducible.
   (d) If R is a PID, then every irreducible element is prime (in particular, all nonzero prime ideals are maximal).
8. Let $J_1 < J_2 < J_3 < \ldots < J_n < \ldots$ be an ascending chain of ideals in a ring R. Show that the join of this chain, $\bigcup_{n=1}^{\infty} J_n$ is also an ideal of R.
9. Write down a complete set of primes for each of the polynomial rings $\mathbb{C}[x]$ and $\mathbb{R}[x]$. How does **(Rgs3)** translate in these two settings?
10. Let $f(x) = c_0 + c_1 x + \ldots + c_r x^r$ be a polynomial of degree r with coefficients $c_i \in \mathbb{Q}$, the field of rational numbers, and let $u \in \mathbb{C}$ be a zero of f. Let $Q[u]$ be the set of all complex numbers of the form $z = d_0 + d_1 u + \ldots + d_{r-1} u^{r-1}$, where $d_i \in \mathbb{Q}$.
    (a) Show that if $y, z \in \mathbb{Q}[u]$, then $y \pm z$ and $yz \in \mathbb{Q}[u]$.
    (b) Show that if f is irreducible in $\mathbb{Q}[x]$, then $\mathbb{Q}[u]$ is a field.
11. Let R be a PID and let $\varphi \colon R \to S$ be an epimorphism of rings. Prove that S is also a PID.
12. Let R be a ring (not necessarily commutative) and suppose that, for each $a \in R$, there is a unique $b \in R$ (depending on a) such that $aba = a$.
    (a) Show that R contains no zero divisors.
    (b) Show that R is a division ring.
13. Define addition and multiplication on the cartesian product $\mathbb{C}^n$ coordinatewise (where $\mathbb{C}$ is field of complex numbers), thus giving it the structure of a ring. Find <u>all</u> ring homomorphisms $\mathbb{C}^n \to \mathbb{C}$.