Throughout this review sheet, $F$ denotes a field.

Proposition: Every ideal in $F[x]$ is a principal ideal, i.e. if $I$ is an ideal in $F[x]$, then there exists an $f(x) \in F[x]$ such that $I = (f(x))$.

Definition: Let $f(x), g(x) \in F[x]$ and assume that not both of $f(x), g(x)$ are zero. A greatest common divisor (gcd) of $f(x)$ and $g(x)$ is a polynomial $d(x)$ such that $d(x) \mid f(x), d(x) \mid g(x)$, and if $e(x)$ is any polynomial such that $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $e(x) \mid d(x)$. A gcd of $f(x)$ and $g(x)$ is unique up to a nonzero constant (and is unique if we require that it is monic).

Proposition: Let $F$ be a field and let $f(x), g(x) \in F[x]$, not both zero. Then a gcd $d(x)$ of $f(x)$ and $g(x)$ exists. Moreover, there exist $p(x), q(x) \in F[x]$ such that $d(x) = f(x)p(x) + g(x)q(x)$. (We say that $d(x)$ is a linear combination of $f(x)$ and $g(x)$.)

Definition: Let $f(x), g(x) \in F[x]$, not both zero. Then $f(x)$ and $g(x)$ are relatively prime if the gcd of $f(x)$ and $g(x)$ is 1.

Corollary: Suppose that $f(x), g(x) \in F[x]$ are relatively prime and that $f(x) \mid g(x)h(x)$. Then $f(x) \mid h(x)$.

Definition: Let $p(x) \in F[x]$. Then $p(x)$ is irreducible in $F[x]$ if $p(x)$ is not 0 or a unit (i.e. is nonconstant) and, for all $f(x) \in F[x]$, if $f(x) \mid p(x)$, then either $f(x)$ is a unit or $f(x) = cp(x)$ for some $c \in F^*$. Clearly $p(x)$ is irreducible if and only if $p(x)$ is nonconstant and, if $p(x) = f(x)g(x)$, one of $f(x), g(x)$ has degree 0 and the other has degree equal to $\deg p(x)$.

Though we usually omit the qualification “in $F[x]$” from the adjective “irreducible,” it is very important, since irreducibility very much depends on the field $F$. For example, $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$, since $x^2 + 1 = (x+i)(x-i)$ in $\mathbb{C}[x]$. A polynomial is reducible if it is not irreducible. A polynomial of degree $n \geq 1$ is reducible if and only if it is a product of two polynomials in $F[x]$ each of which has degree $< n$. A polynomial of degree one is always irreducible. A polynomial of degree two or three is reducible $\iff$ it has a root in $F$. A polynomial of degree four is reducible $\iff$ it has a root in $F$ or is a product of two irreducible polynomials of degree two in $F[x]$.

If $p(x) \in F[x]$ is irreducible and $f(x) \in F[x]$, then either $p(x) \mid f(x)$ or $p(x)$ and $f(x)$ are relatively prime.
Corollary: Let \( p(x) \in F[x] \) be irreducible in \( F[x] \), and suppose that \( p(x) | f(x)g(x) \). Then either \( p(x) | f(x) \) or \( p(x) | g(x) \).

Theorem (Unique factorization in \( F[x] \)): Let \( f(x) \in F[x] \) be a nonconstant polynomial. Then:

(i) There exist irreducible polynomials \( p_1(x), \ldots, p_n(x) \) such that

\[ f(x) = p_1(x) \cdots p_n(x). \]

(ii) This factorization is unique in the following sense: if \( p_i(x), q_j(x) \) are irreducible polynomials such that

\[ p_1(x) \cdots p_n(x) = q_1(x) \cdots q_m(x), \]

then \( n = m \) and, after possibly reordering the \( q_j \), \( p_i(x) = cq_i(x) \) for some \( c \in F^* \).

Theorem: Let \( I \) be an ideal in \( F[x] \). Then the following are equivalent:

1. \( I \) is a maximal ideal.
2. \( I \) is a prime ideal and \( I \neq \{0\} \).
3. \( I = (f(x)) \) for an irreducible polynomial \( f(x) \).

Corollary: The ring \( F[x]/(f(x)) \) is a field if and only if \( f(x) \) is an irreducible polynomial.

Theorem: Let \( F \) be a field and let \( f(x) \) be an irreducible polynomial in \( F[x] \). Then there exists a field \( E \) containing (a subfield isomorphic to) \( F \) and an \( \alpha \in E \) such that \( f(\alpha) = 0 \), in other words there exists a root of \( f(x) \) in \( E \).

In fact, one can take \( E = F[x]/(f(x)) \) and \( \alpha = x + (f(x)) \), identifying \( F \) with the subfield \( \{ a + (f(x)) : a \in F \} \) of \( E \).

Corollary: Let \( F \) be a field and let \( f(x) \) be a nonconstant polynomial in \( F[x] \) (i.e. \( \deg f(x) \geq 1 \)). Then there exists a field \( E \) containing (a subfield isomorphic to) \( F \) and an \( \alpha \in E \) such that \( f(\alpha) = 0 \).

Corollary: Let \( F \) be a field and let \( f(x) \) be a nonconstant polynomial in \( F[x] \) (i.e. \( \deg f(x) = n \geq 1 \)). Then there exists a field \( E \) containing (a subfield isomorphic to) \( F \) and \( \alpha_1, \ldots, \alpha_n \in E \) and \( c \in F \) such that, in \( E[x] \),

\[ f(x) = c(x - \alpha_1) \cdots (x - \alpha_n). \]
Definition: Let $F$ be a field. Then an extension field of $F$ is a field $E$ containing $F$ as a subfield.

Definition: Let $E$ be an extension field of $F$ and let $\alpha \in E$. Then $\alpha$ is algebraic over $F$ if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. The element $\alpha \in E$ is transcendental over $F$, i.e. if $f(x) \in F[x]$ and $f(\alpha) = 0$, then $f(x) = 0$.

Proposition: Let $E$ be an extension field of $F$ and let $\alpha \in E$. Let $ev_\alpha : F[x] \to E$ be the evaluation homomorphism. Then exactly one of the following is true:

(i) $\alpha$ is transcendental over $F$ and $\ker ev_\alpha = \{0\}$. In this case $ev_\alpha$ is an isomorphism from $F[x]$ to the image $\im ev_\alpha = F[\alpha] \subseteq E$. Hence, $F[\alpha]$ is not a subfield of $E$, and $ev_\alpha$ extends to an isomorphism from $F(x)$ to a subfield of $E$, denoted $F(\alpha)$.

(ii) $\alpha$ is algebraic over $F$ and $\ker ev_\alpha \neq \{0\}$. In this case $\ker ev_\alpha = (p(x))$ for an irreducible polynomial $p(x) \in F[x]$, and, for all $f(x) \in F[x]$, $f(\alpha) = 0 \iff p(x) \mid f(x)$. Finally, $\im ev_\alpha = F[\alpha]$ is a subfield of $E$.

Definition: If $E$ is an extension field of $F$ and $\alpha \in E$, we let $F(\alpha)$ be the smallest subfield of $E$ containing $F$ and $\alpha$. In case $\alpha$ is algebraic over $F$, $F(\alpha) = F[\alpha]$. In case $\alpha$ is transcendental over $F$, $F(\alpha) \neq F[\alpha]$, but every element of $F(\alpha)$ can be written as $p(\alpha)/q(\alpha)$, where $p(x), q(x) \in F[x]$ and $q(x) \neq 0$.

Definition: If $E = F(\alpha)$, then $E$ is a simple extension of $F$.

Definition: (i) Let $E$ be an extension field of $F$ and let $\alpha \in E$ be algebraic over $F$. Then $\text{irr}(\alpha, F, x)$ is the unique monic generator of the ideal $\ker ev_\alpha$. It is irreducible and is the monic polynomial of smallest degree for which $\alpha$ is a root.

(ii) With $E, F, \alpha$ as above, we define the degree of $\alpha$ over $F$ (written $\deg_F \alpha$) to be the degree of $\text{irr}(\alpha, F, x)$.

Proposition: Suppose that $E = F(\alpha)$ is a simple extension of $F$, where $\alpha$ is algebraic over $F$ and $\deg_F \alpha = n$. Then every element of $E$ can be uniquely written as $a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1}$ where $a_i \in F$.

Definition: Let $F$ be a field. An $F$-vector space $V$ consists of an abelian group $(V, +)$, whose elements are called vectors, together with a function $F \times V \to V$ called scalar multiplication, and whose value on a pair $(\alpha, v)$ is denoted by $\alpha \cdot v$ or simply $\alpha v$, satisfying the following:
1. For all $\alpha, \beta \in F$ and $v \in V$, $(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$;

2. For all $\alpha \in F$ and $v, w \in V$, $\alpha \cdot (v + w) = (\alpha \cdot v) + (\alpha \cdot w)$;

3. For all $\alpha, \beta \in F$ and $v \in V$, $\alpha \cdot (\beta \cdot v) = (\alpha \beta) \cdot v$;

4. For all $v \in V$, $1 \cdot v = v$.

Proposition: Let $F$ be a field and let $E$ be an extension field of $F$. Then $E$ is an $F$-vector space.

Definition: Let $V$ be an $F$-vector space.

1. A subspace or vector subspace $W$ of $V$ is an abelian subgroup $W$ of $V$ such that, for all $w \in W$ and $\alpha \in W$, $\alpha \cdot w \in W$. With this closure property, $W$ with the induced operations is a vector space in its own right.

2. If $V_1$ and $V_2$ are two $F$-vector spaces, a linear map $F: V_1 \to V_2$ is a homomorphism $F$ of abelian groups such that, for all $\alpha \in F$ and $v \in V_1$, $F(\alpha v) = \alpha F(v)$.

3. Given $v_1, \ldots, v_k \in V$, a linear combination of $v_1, \ldots, v_k$ is an element of $V$ of the form $\sum_{i=1}^{k} \alpha_i v_i$ where $\alpha_1, \ldots, \alpha_k \in F$. The set of all linear combinations of $v_1, \ldots, v_k$, namely

$$\left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in F \right\}$$

is a vector subspace of $V$, called the span of $v_1, \ldots, v_k$. It contains $v_1, \ldots, v_k$ and is the smallest vector subspace of $V$ containing $v_1, \ldots, v_k$.

4. $V$ is finite-dimensional if there exist $v_1, \ldots, v_k \in V$ such that the span of $v_1, \ldots, v_k$ is $V$.

5. $v_1, \ldots, v_k \in V$ are linearly independent if, for all $\alpha_1, \ldots, \alpha_k \in F$, the linear combination $\sum_{i=1}^{k} \alpha_i v_i = 0$ if and only if $\alpha_i = 0$ for all $i$.

6. $v_1, \ldots, v_k \in V$ are a basis for $V$ over $F$, or an $F$-basis, or simply a basis if $F$ is clear from the context, if they are linearly independent and span $V$. $v_1, \ldots, v_k \in V$ are a basis for $V$ over $F$ if and only if every $v \in V$ can be written as $\sum_{i=1}^{k} \alpha_i v_i = 0$ for a unique choice of $\alpha_1, \ldots, \alpha_k \in F$. 

4
Theorem: Let \( V \) be an \( F \)-vector space. Suppose that \( v_1, \ldots, v_k \in V \) are linearly independent and that \( w_1, \ldots, w_\ell \in V \) span \( V \). Then \( k \leq \ell \).

Corollary: If \( V \) is finite dimensional, then there exists a basis for \( V \). Moreover, every two bases have the same number of elements, and this number is called the dimension \( \dim_F V \) of \( V \).

Corollary: If \( V \) is finite dimensional and \( v_1, \ldots, v_k \in V \) are linearly independent, then \( v_1, \ldots, v_k \) can be completed to a basis of \( V \): there exist \( v_{k+1}, \ldots, v_n \) such that \( v_1, \ldots, v_n \) are a basis of \( V \). In particular, \( k \leq \dim_F V \).

Definition: Suppose that \( E \) is an extension field of \( F \). If \( E \) is a finite-dimensional \( F \)-vector space, then \( E \) is called a finite extension of \( F \). (Note: this does not mean that \( E \) is a finite set.) In this case, \( \dim_F E \) is called the degree of \( E \) over \( F \) and is written \( [E : F] \).

Proposition: Suppose that \( E = F(\alpha) \) is a simple extension of \( F \). Then \( E \) is a finite extension of \( F \) if and only if \( \alpha \) is algebraic over \( F \). In this case \( [F(\alpha) : F] = \dim_F F(\alpha) = \deg_F \alpha \) and \( 1, \alpha, \ldots, \alpha^{n-1} \) is a basis of \( E \), where \( n = \deg_F \alpha \).

Proposition: Let \( E \) be an extension field of \( F \), and suppose that \( E \) is a finite dimensional vector space over \( F \), of dimension \( \dim_F E = [E : F] \). Let \( V \) be an \( E \)-vector space; note that we can also view \( V \) as an \( F \)-vector space. Then \( V \) is finite dimensional as an \( E \)-vector space if and only if \( V \) is finite dimensional as an \( F \)-vector space, and in this case

\[
\dim_F V = [E : F] \dim_E V.
\]

Corollary: Let \( E \) be an extension field of the field \( F \) and let \( K \) be an extension field of \( E \), i.e. \( F \leq E \leq K \). Then \( K \) is a finite extension of \( F \) if and only if \( K \) is a finite extension of \( E \) and \( E \) is a finite extension of \( F \), and in this case we have

\[
[K : F] = [K : E][E : F].
\]

Corollary: Let \( E \) be an extension field of the field \( F \) and let \( K \) be an extension field of \( E \), i.e. \( F \leq E \leq K \), and suppose that \( K \) is a finite extension of \( F \). Then \( K \) is a finite extension of \( E \) and \( E \) is a finite extension of \( F \), and in this case \([K : E]\) and \([E : F]\) both divide \([K : F]\).

Notation: if \( E \) is an extension field of \( F \), and \( \alpha, \beta \in E \), then \( F(\alpha, \beta) \) is the smallest subfield of \( E \) containing \( F, \alpha, \) and \( \beta \). Clearly \( F(\alpha, \beta) = F(\alpha)(\beta) = F(\beta)(\alpha) \). The field \( F(\alpha_1, \ldots, \alpha_n) \) is defined similarly.
Definition: if \( E \) is an extension field of \( F \), then \( E \) is an algebraic extension of \( F \) if, for every \( \alpha \in E \), \( \alpha \) is algebraic over \( F \).

Proposition: If \( E \) is a finite extension of \( F \), then \( E \) is an algebraic extension of \( F \).

Proposition-Definition: Let \( E \) be an extension field of \( F \), and let \( \alpha, \beta \in E \). If \( \alpha \) and \( \beta \) are algebraic over \( F \), then so are \( \alpha \pm \beta \), \( \alpha \beta \), and \( \alpha/\beta \) (if \( \beta \neq 0 \)). Thus the subset \( \{ \alpha \in E : \alpha \text{ is algebraic over } F \} \) is a subfield of \( E \), the algebraic closure of \( F \) in \( E \).

Definition: The algebraic closure of \( \mathbb{Q} \) in \( \mathbb{C} \) is a subfield of \( \mathbb{C} \), denoted by \( \overline{\mathbb{Q}} \) or by \( \mathbb{Q}^{\text{alg}} \). It is called the field of algebraic numbers.

Lemma: Let \( E \) be an extension field of \( F \). Then \( E \) is a finite extension of \( F \) \( \iff \) there exist \( \alpha_1, \ldots, \alpha_n \in E \), algebraic over \( F \), such that \( E = F(\alpha_1, \ldots, \alpha_n) \).

Corollary: Let \( F \leq E \leq K \) with \( E \) an algebraic extension of \( F \). If \( \alpha \in K \) and \( \alpha \) is algebraic over \( E \), then \( \alpha \) is algebraic over \( F \).

Corollary: Let \( F \leq E \leq K \). Then \( K \) is an algebraic extension of \( F \) \( \iff \) \( K \) is an algebraic extension of \( E \) and \( E \) is an algebraic extension of \( F \).

Definition: Let \( K \) be a field. Then \( K \) is algebraically closed if, for every \( f(x) \in K[x] \) of degree at least one, there exists \( \alpha \in K \) such that \( f(\alpha) = 0 \).

Proposition: Let \( K \) be a field. Then the following are equivalent:

1. \( K \) is algebraically closed.
2. If \( f(x) \in K[x] \) and \( \deg f(x) \geq 1 \), then \( f(x) \) is a product of linear factors.
3. If \( L \) is an algebraic extension of \( K \), then \( L = K \).

Famous fact (Fundamental Theorem of Algebra): \( \mathbb{C} \) is algebraically closed.

Definition: An algebraic closure of \( F \) is an extension field \( K \) of \( F \) such that (i) \( K \) is algebraically closed and (ii) \( K \) is algebraic over \( F \).

Proposition: Let \( F \) be a field and let \( E \) be an extension field of \( F \) which is algebraically closed. Then the algebraic closure of \( F \) in \( E \) is an algebraic closure of \( F \).

Corollary: \( \mathbb{Q}^{\text{alg}} \) is algebraically closed, and is an algebraic closure of \( \mathbb{Q} \).

Fact (Existence of Algebraic Closures): Let \( F \) be a field. Then there exists an extension field \( E \) of \( F \) which is an algebraic closure of \( F \). Moreover, two algebraic closures of \( F \), say \( E_1 \) and \( E_2 \), are isomorphic; more precisely, there exists an isomorphism \( \sigma: E_1 \to E_2 \) such that \( \sigma(a) = a \) for all \( a \in F \).
Definition: For \( f(x) = \sum_{i=0}^{n} a_i x^i \in F[x] \), the formal derivative \( Df(x) \) of the polynomial is the polynomial \( Df(x) = \sum_{i=1}^{n}(i \cdot a_i)x^{i-1} \in F[x] \). It satisfies:

1. \( D: F[x] \to F[x] \) is \( F \)-linear, i.e. for all \( f, g \in F[x] \) and \( a \in F \),
   \[ D(f + g) = Df + Dg \text{ and } D(af) = aDf. \]

2. (Product rule) For all \( f, g \in F[x] \), \( D(fg) = (Df)g + f(Dg) \).

3. (Power rule) For all \( f \in F[x] \) and \( n \in \mathbb{N} \), \( D(f^n) = n \cdot f^{n-1}Df \).

4. If \( F \) has characteristic \( p \), then \( D(x^p) = 0 \). In general, if \( F \) has characteristic \( 0 \), then \( Df(x) = 0 \iff f(x) \) is constant. If \( F \) has characteristic \( p \), then \( Df(x) = 0 \), where \( f(x) = \sum_{i=0}^{n} a_i x^i \), \( \iff \) for all \( i \) such that \( a_i \neq 0 \), \( p|a_i \), \( f(x) = \sum_{j=0}^{m} a_{jp} x^{jp} \), \( \iff f(x) = g(x^p) \), where \( g(x) = \sum_{j=0}^{m} b_j x^{j} \) (we set \( b_j = a_{jp} \)).

We can restate (4) as: \( \text{Ker } D = F \) if the characteristic of \( F \) is 0, and \( \text{Ker } D = F[x^p] \) if the characteristic of \( F \) is \( p > 0 \).

Proposition: \( a \) is a multiple root of \( f(x) \) (i.e. \( (x - a)^m \mid f(x) \) for some \( m \geq 2 \)) \( \iff f(a) = Df(a) = 0 \).

Lemma: Let \( E \) be an extension field of \( F \), and let \( f(x), g(x) \in F[x] \subseteq E[x] \).

(i) \( f(x) \) divides \( g(x) \) in \( F[x] \iff f(x) \) divides \( g(x) \) in \( E[x] \).

(ii) Let \( d(x) \in F[x] \). Then \( d(x) \) is a gcd of \( f(x) \) and \( g(x) \) in \( F[x] \iff d(x) \) is a gcd of \( f(x) \) and \( g(x) \) in \( E[x] \).

(iii) \( f(x) \) and \( g(x) \) are relatively prime in \( F[x] \iff f(x) \) and \( g(x) \) are relatively prime in \( E[x] \).

Proposition: Let \( f(x) \in F[x] \). Then \( f(x) \) and \( Df(x) \) are not relatively prime \( \iff \) there exists an extension field \( E \) of \( F \) such that \( f(x) \) has a multiple root in \( E \).

Corollary: Let \( f(x) \in F[x] \) be an irreducible polynomial. Then \( f(x) \) has a multiple root in some extension field \( E \) of \( F \iff Df(x) = 0 \). In particular, if the characteristic of \( F \) is zero, \( f(x) \) does not have a multiple root in any extension field \( E \) of \( F \).

Let \( \mathbb{F} \) be a finite field. Then \( \mathbb{F} \) has characteristic \( p > 0 \), \( p \) a prime number, and the field \( \mathbb{Z}/p\mathbb{Z} \), which we will write henceforth as \( \mathbb{F}_p \), is a subfield of...
\( \mathbb{F} \). Since \( \mathbb{F} \) is finite, it is a finite-dimensional \( \mathbb{F}_p \)-vector space, of dimension \( n = [\mathbb{F} : \mathbb{F}_p] \), say. Thus \( \#(\mathbb{F}) = q = p^n \) is a prime power. Also, since \( \mathbb{F}^* \) is a finite subgroup of \( \mathbb{F}^* \), it is cyclic, say \( \mathbb{F}^* = \langle \alpha \rangle \), and so \( \mathbb{F} = \mathbb{F}_p(\alpha) \). More generally, if \( \mathbb{F}' \) is any subfield of \( \mathbb{F} \), then \( \mathbb{F} = \mathbb{F}'(\alpha) \). In particular, every finite extension of a finite field is a simple extension.

Definition: For a finite field \( \mathbb{F} \) of characteristic \( p \) (i.e. \( \#(\mathbb{F}) \) is a power of \( p \)), let \( \sigma_p : \mathbb{F} \to \mathbb{F} \) be the Frobenius homomorphism: \( \sigma_p(\alpha) = \alpha^p \). Since \( \mathbb{F} \) is finite and \( \sigma_p \) is injective, it is also surjective, hence an automorphism of \( \mathbb{F} \) with the property that \( \sigma_p(a) = a \) for all \( a \in \mathbb{F}_p \leq \mathbb{F} \). More generally, for a positive integer, we can define \( \sigma_{p^k}(\alpha) = \alpha^{p^k} \). By induction, we claim that \( \sigma_{p^k}(\alpha) = (\sigma_p)^k(\alpha) = \sigma_p(\sigma_p(\alpha)) = \sigma_p(\sigma_p(\alpha)) = \cdots = \sigma_p(\alpha_{p^{k-1}}) = (\alpha_{p^{k-1}})^p = \alpha^{p^k} = \sigma_{p^k}(\alpha) \). Thus \( \sigma_{p^k} \) is also an automorphism of \( \mathbb{F} \). In particular, for \( q = p^n = \#(\mathbb{F}) \), \( \sigma_q \) is an automorphism of \( \mathbb{F} \). If \( \mathbb{F} \) is a field with \( \#(\mathbb{F}) = q = p^n \), then, for all \( \alpha \in \mathbb{F} \), \( \alpha^q = \alpha \). Two equivalent formulations are (a) \( \alpha \) is a root of \( x^q - x \); (b) \( \sigma_q(\alpha) = \alpha \).

Theorem: Let \( p \) be a prime number.

(i) For every \( n \in \mathbb{N} \), if we set \( q = p^n \), then there exists a field \( \mathbb{F}_q \) with \( \#(\mathbb{F}_q) = q \).

(ii) If \( \mathbb{F}_1 \) and \( \mathbb{F}_2 \) are two finite fields with \( \#(\mathbb{F}_1) = \#(\mathbb{F}_2) \), then \( \mathbb{F}_1 \) and \( \mathbb{F}_2 \) are isomorphic.

(iii) Let \( \mathbb{F} \) be a field of order \( q = p^n \), and let \( \mathbb{F}' \) be a field of order \( q' = p^{m'n} \). Then \( \mathbb{F}' \) is isomorphic to a subfield of \( \mathbb{F} \) \( \iff \) \( m|n \) \( \iff \) \( q = (q')^d \) for some positive integer \( d \).

From now on in this review sheet, \( R \) denotes an integral domain. For \( r, s \in R \), we say that \( r \) divides \( s \) (written \( r|s \)) if there exists a \( t \in R \) such that \( s = rt \). We have defined units for \( R \), and the (multiplicative) group of all such is denoted \( R^* \). If \( r, s \in R \), then \( r \) and \( s \) are associates if there exists a unit \( u \in R^* \) such that \( r = us \). In this case, \( s = u^{-1}r \), and indeed the relation that \( r \) and \( s \) are associates is an equivalence relation. We say that \( r \in R \) is irreducible if \( r \neq 0 \), \( r \) is not a unit, and if \( s \) divides \( r \) then either \( s \) is a unit or \( s \) is an associate of \( r \). In other words, if \( r = st \) for some \( t \in R \), then either \( s \) or \( t \) is a unit (and hence the other is an associate of \( r \)).

Definition: \( R \) is a unique factorization domain (UFD) if (i) for every \( r \in R \) not 0 or a unit, there exist irreducibles \( p_1, \ldots, p_n \in R \) such that \( r = p_1 \cdots p_n \), and (ii) if \( p_i, 1 \leq i \leq n \) and \( q_j, 1 \leq j \leq m \) are irreducibles such
that $p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and, after reordering, $p_i$ and $q_j$ are associates.

Definition: $R$ is a principal ideal domain (PID) if every ideal $I$ of $R$ is principal, i.e. for every ideal $I$ of $R$, there exists $r \in R$ such that $I = (r)$.

Theorem (not proved): A principal ideal domain is a unique factorization domain.

Definition: Let $R$ be an integral domain. Let $r, s \in R$, not both 0. A greatest common divisor (gcd) of $r$ and $s$ is an element $d \in R$ such that $d|r$, $d|s$, and if $e \in R$ and $e|r$, $e|s$, then $e|d$. If a gcd of $r$ and $s$ exists, it is unique up to a unit (i.e. any two gcd’s of $r$ and $s$ are associates). The elements $r$ and $s$ are relatively prime if gcd$(r, s) = 1$; equivalently, if $d \in R$ and $d|r$, $d|s$, then $d$ is a unit.

Proposition: if $R$ is a UFD, then the gcd of two elements $r, s \in R$, not both 0, exists.

Theorem: Let $R$ be a PID, and let $r, s \in R$, not both 0. Then the gcd $d$ of $r$ and $s$ exists. Moreover, $d$ is a linear combination of $r$ and $s$: there exist $a, b \in R$ such that $d = ar + bs$.

Note: for a general UFD, the gcd of two elements $r$ and $s$ will not in general be a linear combination of $r$ and $s$.

Corollary (of Theorem): If $R$ is a PID, $r, s \in R$ are relatively prime and $r|st$, then $r|t$.

Corollary: If $R$ is a PID, and $r \in R$ is an irreducible, then for all $s, t \in R$, if $r|st$, then either $r|s$ or $r|t$.

The two corollaries above are true more generally in a UFD, with fairly straightforward proofs.

The following proves the uniqueness half of the assertion that a PID is a UFD:

Corollary: If $R$ is a PID, then uniqueness of factorization holds in $R$: if $p_i, 1 \leq i \leq n$ and $q_j, 1 \leq j \leq m$ are irreducibles such that $p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and, after reordering, $p_i$ and $q_j$ are associates.

Definition: Let $R$ be an integral domain. A Euclidean norm on $R$ is a function $N: R - \{0\} \to \mathbb{Z}$ satisfying:

1. For all $r \in R - \{0\}$, $N(r) \geq 0$.

2. For all $a, b \in R$ with $a \neq 0$, there exist $q, r \in R$ with $b = aq + r$ and either $r = 0$ or $N(r) < N(a)$. 


An integral domain $R$ such that there exists a Euclidean norm on $R$ is called a \textit{Euclidean domain}.

Definition: The Euclidean norm $N$ is \textit{submultiplicative} if in addition $N$ satisfies: For all $a, b \in R - \{0\}$, $N(a) \leq N(ab)$. It is \textit{multiplicative} if $N$ satisfies: For all $a, b \in R - \{0\}$, $N(ab) = N(a)N(b)$. If $N$ is multiplicative and $N(a) > 0$ for all $a \in R - \{0\}$, then $N$ is submultiplicative.

Examples: $R = \mathbb{Z}$, $N(a) = |a|; R = F[x]$, $F$ a field, and $N(f(x)) = \text{deg } f(x)$, defined for $f(x) \neq 0$. Here (1) is clear and (2) is the statement of long division in $\mathbb{Z}$ or in $F[x]$. In fact, it is easy to see that $N$ is submultiplicative in both cases.

Proposition: If $R$ is a Euclidean domain, then $R$ is a PID.

Lemma: Let $R$ be an integral domain and let $N$ be a submultiplicative Euclidean norm on $R$. For all $b \in R - \{0\}$, exactly one of the following holds:

1. $b$ is not a unit and $N(a) < N(ab)$ for all $a \in R - \{0\}$.
2. $b$ is a unit and $N(a) = N(ab)$ for all $a \in R - \{0\}$.

Proposition: If $R$ is a Euclidean domain with a submultiplicative Euclidean norm and $r \in R$ is not 0 or a unit, then $r$ is a product of irreducibles.

Corollary: If $R$ is a Euclidean domain, then $R$ is a UFD.

(Of course, this follows from the more general fact that a PID is a UFD.)