1. Group action; Definition and first theorems:

1.1. Definition. We start by recalling the notion of an equivalence relation. Let \(A\) be a set. A relation \(R\) on \(A\) is a subset of \(A \times A\). If \((a, b) \in R\) then we write \(aRb\) and we say that \(a\) is related to \(b\) via the relation \(R\). We simply say \(a\) is related to \(b\) if the relation \(R\) is understood from context.

Let \(A\) be a set and \(R\) be a relation on \(A\). We say that \(R\) is an equivalence relation on \(A\) if \(R\) satisfies the following three conditions: (i) \(aRa\) for all \(a \in A\), (ii) If \(aRb\), then \(bRa\) for all \(a, b \in A\), (iii) If \(aRb\) and \(bRc\), then \(aRc\) for all \(a, b, c \in A\).

Let \(R\) be an equivalence relation on a set \(A\). If \(a \in A\), we define the equivalence class of \(a\) to be the set of all \(b \in A\) such that \(a\) is related to \(b\). Verify that:

○ If two elements \(a, b \in A\) are related, then their equivalence classes are identical, otherwise their equivalence classe are disjoint.
○ Members of the same equivalence class are all related to each other and members of distinct equivalence classes are never related to each other.
○ The set \(A\) is the disjoint union of all the equivalence classes.

1.2. Definition. Let \(G\) be a group with identity element \(e\) and \(A\) be a set. A left action of \(G\) on \(A\) is a map \(\rho : G \times A \to A\) such that \(\rho(e, a) = a\) for all \(a \in A\) and \(\rho(g, \rho(h, a)) = \rho(gh, a)\) for all \(g, h \in G\) and \(a \in A\). Usually we shall use the notation \(\rho(g, a) = g.a\). So we have \(e.a = a\) for all \(a \in A\) and \(g.(h.a) = (gh).a\), for all \(a \in A\) and for all \(g, h \in G\).

1.3. Exercise. Show that specifying an action of \(G\) on \(A\) is equivalent to having a group homomorphism from \(G\) to \(\text{Aut}(A)\), the group of all one to one and onto maps from \(A\) to \(A\).

1.4. Definition. Suppose \(G\) acts on \(A\). If \(a, b \in A\), we write \(a \sim_G b\) if there exists \(g \in G\) such that \(ga = b\). Verify that \(\sim_G\) is an equivalence relation on \(A\). The equivalence class of \(a \in A\) is called the orbit of \(a\) under \(G\) and is denoted by \(\mathcal{O}_a\). So

\[\mathcal{O}_a = \{b \in A: b = ga \text{ for some } g \in G\}\]

We write \((G\setminus A)\) for the set of orbits. Since \(\sim_G\) is an equivalence relation, \(A\) is the disjoint union of the orbits, that is,

\[A = \bigsqcup_{\mathcal{O} \in G \setminus A} \mathcal{O},\]

where \(\bigsqcup\) denotes disjoint union. This is called the orbit decomposition of \(A\). For \(a \in A\), let

\[G_a = \{g \in G: ga = a\}\]

Verify that \(G_a\) is a subgroup of \(G\). The subgroup \(G_a\) is called the stabilizer of \(a\) in \(G\).

1.5. Theorem (Lagrange). Let \(H\) be a subgroup of a group \(G\). Consider \(H\) acting on \(G\) by left multiplication: \(H \times G \to G\) given by \((h, g) \mapsto hg\). The orbit of \(g \in G\) is the set \(Hg = \{hg: h \in H\}\). These orbits are called the right cosets of \(H\) in \(G\). The set of right cosets of \(H\) in \(G\) is denoted by \(H \setminus G\). The group \(G\) is the disjoint union of the right cosets of \(H\). If \(G\) is finite, then one has \(|G| = |H||H \setminus G|\).

Proof. Consider \(H\) acting on \(G\) by left multiplication. From orbit decomposition, we get that \(G\) is a disjoint union of the right cosets:

\[G = \bigsqcup_{\mathcal{O} \in H \setminus G} \mathcal{O}.\]
Verify that each coset of $H$ in $G$ has the same cardinality, namely $|H|$. If $G$ is finite, it follows that $|G| = |H||H\backslash G|$. \hfill \Box

1.6. Definition/Remark: Let $G$ be a group and $A$ be a set. A right action of $G$ on $A$ is a map $A \times G \to A$ written $(a, g) \mapsto a.g$ such that $a.e = a$ and $(a.g).h = a.(gh)$ for all $a \in A$ and $g, h \in G$. If $G$ acts on $A$ on the right, then the set of orbits will be denoted by $A/G$. Everything we said about left action carries over verbatim for right actions.

If $H$ is a subgroup of $G$, then there is also a right action of $H$ on $G$ via right multiplication: $G \times H \to G$ given by $(g, h) \mapsto gh$. The orbits have the form $gH$ for $g \in G$ and are called left cosets of $H$ in $G$. So the set of left cosets of $H$ in $G$ is denoted by $G/H$. The obvious analog of theorem 1.5 holds for the set of left cosets.

When we say $G$ acts on $A$, we shall mean $G$ acts on the left, unless otherwise specified.

1.7. Theorem ( Orbit-Stabilizer theorem). Let $G$ be a group acting on a set $A$. Fix $a \in A$. Then one has a bijection $G/G_a \simeq \mathcal{O}_a$. In particular $|G| = |G_a||\mathcal{O}_a|$. So $G$ is finite if and only if $G_a$ and $\mathcal{O}_a$ are finite for some $a \in A$.

Proof. Consider the map $\varphi : G \to \mathcal{O}_a$ given by $\varphi(g) = ga$. By definition of orbit, this is an onto map from $G$ to $\mathcal{O}_a$.

Claim: If $g \in G$, then $\varphi^{-1}(ga) = gG_a$. The verification is routine:

$$h \in \varphi^{-1}(ga) \iff \varphi(h) = ga \iff ha = ga \iff g^{-1}ha = a \iff g^{-1}h \in G_a \iff h \in gG_a.$$ 

Note that each element $b \in \mathcal{O}_a$ have the form $b = ga$ for some $g \in G$, so for each such $b \in \mathcal{O}_a$, the preimage $\varphi^{-1}(b)$ is a left coset of $G_a$ in $G$. Thus we have the map $\Phi : \mathcal{O}_a \to G/G_a$ given by $\Phi(b) = \varphi^{-1}(b)$. Verify that $\Phi : \mathcal{O}_a \to G/G_a$ is one to one and onto. In particular $|G/G_a| = |\mathcal{O}_a|$. Now Lagrange’s theorem (i.e. the analog of theorem 1.5 for left cosets) implies that $|G_a||\mathcal{O}_a| = |G_a||G/G_a| = |G|$. \hfill \Box

1.8. Example. Let $G$ be a group and $g, h \in G$. Define $c_g(h) = ghg^{-1}$. The operation $g \mapsto ghg^{-1}$ is called conjugating $h$ by $g$. Verify that the map $G \times G \to G$ given by $(g, h) \mapsto c_g(h)$ is a left action of $G$ on $G$, this is called the conjugation action. Consider $G$ acting on $G$ by conjugation. The orbit of an element $a \in G$ under this action consists of all the elements of the form $gag^{-1}$, where $g$ varies over $G$. This orbit is called the conjugacy class of $a$, and we shall denote it by Class$(a)$. The orbit decomposition implies that the $G$ is the disjoint union of all the conjugacy classes.

Let $a \in G$. The stabilizer of $G$ under the conjugation action is $\{g \in G : gag^{-1} = a\}$. This subgroup is called the centralizer of $a$ in $G$ and is denoted by $C_G(a)$. Now assume that $G$ is finite. Then the orbit stabilizer theorem implies that for each $a \in G$, we have $|G| = |C_G(a)||\text{Class}(a)|$.

Recall that the center of $G$, denoted $Z(G)$, consists of all the elements $z \in G$ such that $zg = gz$ for all $g \in G$. Let $Z(G) = \{z_1, \ldots, z_m\}$. In other words, $\{z_1\}, \ldots, \{z_m\}$ are precisely the one element conjugacy classes in $G$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the rest of the conjugacy classes and choose $a_1 \in \mathcal{O}_1, \ldots, a_r \in \mathcal{O}_r$, so $\mathcal{O}_j = \text{Class}(a_j)$. We say that $a_j$ is a representative for the conjugacy class $\mathcal{O}_j$. Now from orbit decomposition, we get that $G$ is a disjoint union of
the sets \{z_1\}, \ldots, \{z_m\}, \text{Class}(a_1), \ldots, \text{Class}(a_r). \text{ So}

\[ |G| = |Z(G)| + \sum_{j=1}^{r} |\text{Class}(a_j)|. \]

Using the orbit stabilizer theorem we get, the class equation:

\[ |G| = |Z(G)| + \sum_{j=1}^{r} \frac{|G|}{|C_G(a_j)|}. \]
2. Sylow’s theorems

For this section, let $p$ be a prime number. A $p$-group is a finite group whose order is a power of $p$. Let $G$ be a finite group. Let $p^n$ be the largest power of $p$ that divides $|G|$. Then a subgroup of $G$ of order $p^n$ is called a Sylow $p$-subgroup of $G$. Let $\text{Syl}_p(G)$ denote the set of all Sylow $p$-subgroups of $G$.

2.1. Lemma. Let $H$ be a $p$-group acting on a set $X$. Let $X_H$ be the set of points of $X$ that are fixed by the action of $H$. Then $|X_H| \equiv |X| \mod p$.

\textit{Sketch of proof.} Note that $X_H$ is precisely the union of the single element orbits. Since $H$ is a $p$-group, the orbit-stabilizer theorem implies that the size of each non-singleton orbit is a power of $p$. Now the lemma follows from the orbit decomposition of $X$. \hfill $\square$

2.2. Theorem (Sylow’s theorem). Let $G$ be a finite group whose order is divisible by $p$.

(a) $G$ has a Sylow $p$-subgroup.

(b) Let $H$ be a $p$-subgroup of $G$ and $P \in \text{Syl}_p(G)$. Then there exists $g \in G$ such that $gHg^{-1} \subseteq P$. In particular, all the Sylow $p$-subgroups of $G$ are conjugate to each other.

(c) If $p^n$ is the highest power of $p$ that divides $|G|$, then $|\text{Syl}_p(G)|$ divides $|G|/p^n$. Also $|\text{Syl}_p(G)| \equiv 1 \mod p$.

\textit{Proof.} (a) Let $|G| = p^nm$ where $m$ is relatively prime to $p$. Let $A$ be the set of all subsets of $G$ of order $p^n$. Consider the action of $G$ on $A$ by left multiplication. One has

$$|A| = \binom{p^nm}{p^n} = \frac{p^nm}{p^n} \cdot \frac{p^nm - 1}{p^n - 1} \cdot \frac{p^nm - 2}{p^n - 2} \cdots \frac{p^nm - (p^n - 1)}{p^n - (p^n - 1)} = m \prod_{j=1}^{p^n-1} \frac{p^nm - j}{p^n - j}.$$  

Observe that for each $j$ such that $1 \leq j < p^n$, the integers $(p^nm - j)$ and $(p^n - j)$ are divisible by exactly the same power of $p$, namely the power of $p$ that divides $j$. It follows that $|A|$ is not divisible by $p$. From orbit decomposition of $A$, it follows that there must be an orbit $O$ in $A$ whose size is relatively prime to $p$. Pick $S \in O$ and pick $x \in S$. Let $P = x^{-1}S$. Then $P$ and $S$ are in the same orbit $O$ and $P$ contains the identity element of $G$. Let $G_P$ be the stabilizer of $P$. By the orbit-stabilizer theorem, $p^n \cdot m = |G| = |G_P||O|$, so $p^n$ divides $|G_P|$. On the other hand, if $g \in G_P$, then $gP = P$, in particular $g = g.e \in P$, so $G_P \subseteq P$. Since $P$ has size $p^n$, it follows that $G_P = P$, so $P$ is a Sylow $p$-subgroup of $G$.

(b) Let $G/P$ be the set of left cosets of $P$ in $G$. Consider the action of $H$ on $G/P$ by left translation. Since $|G/P| = |G|/|P| = m$ is relatively prime to $p$, lemma 2.1 implies that there exists an element of $G/P$, call it $gP$, fixed by $H$. In other words, there exists $g \in G$ such that $hgP = gP$ for all $h \in H$, so $g^{-1}Hg \subseteq P$. If $H \subseteq \text{Syl}_p(G)$, then it follows that there exists $g \in G$ such that $g^{-1}Hg = P$, so all the Sylow $p$-subgroups are conjugate.

(c) Let $G$ act on $\text{Syl}_p(G)$ by conjugation. Let $P \in \text{Syl}_p(G)$. Part (b) implies that the orbit of $P$ is $\text{Syl}_p(G)$ and the stabilizer of $P$ is the subgroup $N_G(P) := \{g \in G : gPg^{-1} = P\}$. So $|\text{Syl}_p(G)| = |G|/|N_G(P)|$. Since $P \subseteq N_G(P)$, it follows that $|\text{Syl}_p(G)|$ is a factor of $|G|/p^n$.

Now let $P$ act on $\text{Syl}_p(G)$ by conjugation. We claim that there is only one element of $\text{Syl}_p(G)$ fixed by this action of $P$, namely $P$ itself. To say that $Q \in \text{Syl}_p(G)$ is fixed by the action of $P$ means $gQg^{-1} = Q$ for all $g \in P$, that is $P \subseteq N_G(Q)$. But $Q$ is normal in $N_G(Q)$, so part (b) implies that $Q$ is the only Sylow $p$-subgroup inside $N_G(Q)$; it follows that $Q = P$. This proves the claim. Lemma 2.1 now implies that $|\text{Syl}_p(G)| \equiv 1 \mod p$. \hfill $\square$
Sylow’s theorem are often used to detect (normal) subgroups in finite groups, which in turn help in understanding the structure of finite groups and classifying them. For example part (c) of Sylow’s theorem can sometimes be used to show that $G$ has a unique Sylow $p$-subgroup for certain prime $p$. And if $G$ has a unique Sylow $p$-subgroup, then it must be normal because any conjugate of it would also be a Sylow $p$-subgroup. Recall the following facts:

- Let $P$ and $Q$ be subgroups of $G$ such that $P$ normalizes $Q$. Then there is a homomorphism $P \to \text{Aut}(Q)$ given by $x \mapsto c_x$, where $c_x : Q \to Q$ is given by $c_x(q) = xqx^{-1}$.
- $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Proof: Verify that for each $x \in (\mathbb{Z}/p\mathbb{Z})^*$, we have an automorphism $L_x \in \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ given by $L_x(k) = kx$. Verify that this gives an injective homomorphism from $L : (\mathbb{Z}/p\mathbb{Z})^* \to \text{Aut}(\mathbb{Z}/p\mathbb{Z})$, defined by $L(x) = L_x$.

Let $f$ be an automorphism of $\mathbb{Z}/7\mathbb{Z}$. Then $f(k) = kf(1)$; so the map $f$ is determined by $f(1)$, and $f(1) \not= 0$, so $f(1) \in (\mathbb{Z}/p\mathbb{Z})^*$. So $f = L_{f(1)}$, so $L$ is an isomorphism.

- Let $P$ and $Q$ be subgroups of $G$. Then $PQ$ is a subgroup of $G$ if and only if $PQ =QP$. Also $|PQ| = |P||Q|/|P \cap Q|$. (If either $P$ or $Q$ is normal then this follows from the second isomorphism theorem. In general see the book).

- Let $P$ and $Q$ be subgroups of $G$. If $P$ and $Q$ commute and $PQ = G$ and $P \cap Q = \{e\}$, then $G$ is the internal direct product of $P$ and $Q$, in particular, $G \cong P \times Q$. proof: Since $P$ and $Q$ commute and $PQ = G$, both $P$ and $Q$ are normal in $G$. By second isomorphism theorem we get $G/P \cong PQ/P \cong Q/P \cap Q \cong Q$ and similarly $G/Q \cong P$. By universal property of direct product, we have map $G \mapsto G/P \times G/Q$ given by $(g \mapsto (g \mod P, g \mod Q))$ whose kernel is $P \cap Q = \{e\}$, so we have an one to one homomorphism $G \to Q \times P$, but $|G| = |P||Q|/|P \cap Q| = |P||Q|$, so the one to one homomorphism $G \to P \times Q$ must be onto as well.

2.3. Classify the groups of order 175: Let $G$ be a group of order 175. Let $n_5$ denote the Sylow $p$-subgroups in $G$. Then $n_5 \equiv 1 \mod 5$ and $n_5$ divides $175/25 = 7$. It follows that $n_5 = 1$, so $G$ has a unique Sylow 5-subgroup $P$ of order 25; so $P$ must be normal. Similar argument shows that $G$ has a unique Sylow 7 subgroup $Q \cong \mathbb{Z}/7\mathbb{Z}$. If $x \in P \setminus \{e\}$, then $x \mapsto c_x$ gives a homomorphism from $P \to \text{Aut}(Q) \cong (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$. Since $P$ has order 25 which is relatively prime to 6, this homomorphism must be trivial, which implies $P$ and $Q$ commute; also an element in $P \cap Q$ would have order divisible by both 25 and 7, so $P \cap Q = \{e\}$.

It follows that $|PQ| = |P||Q|/|P \cap Q| = 175$, so $PQ = G$. Since $P \cap Q = \{e\}$ and $P$ and $Q$ commute, it follows that $G$ is the direct product of $P$ and $Q$, so $G \cong P \times Q$.

It remains to analyse the possible structures of $P$. If $P$ has an element of order 25, then $P \cong \mathbb{Z}/25\mathbb{Z}$. Suppose not. Then every non-identity element of $P$ has order 5. Since $P$ is a $p$-group, it has a nontrivial center, so it has a central element $x$ of order 5. Let $y$ be a non-identity element in $\langle x \rangle$. Then $\langle x \rangle$ and $\langle y \rangle$ are two commuting $\mathbb{Z}/5\mathbb{Z}$’s in $P$ and their intersection has is trivial; because otherwise the intersection would have size 5, which would mean $\langle x \rangle = \langle y \rangle$, in particular $y \in \langle x \rangle$, contrary to our assumption. It follows that $P$ is the internal direct product of $\langle x \rangle$ and $\langle y \rangle$, so $P \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

To summarize, there are two possibilities for isomorphism type of $G$: $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $(\mathbb{Z}/5)^2 \times \mathbb{Z}/7$. These two groups are non-isomorphic because the first one has an element of order 25, while the second one does not.
A quick run through definitions of some basic algebraic structures.

Let $S$ be a set. A binary operation $\cdot$ on $S$ is a function $\cdot : S \times S \to S$. Often we denote this binary operation as simply by a dot and we write $\cdot(a, b) = a \cdot b$ for $a, b \in S$.

Let $(S, \cdot)$ be a set $S$ with a binary operation, denoted by $\cdot$. We say that the binary operation $\cdot$ is associative if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$. An element $e \in S$ is called an identity of $S$ if $e \cdot a = a \cdot e = a$ for all $a \in S$. Sometimes the identity of $S$ is denoted by $1$ instead of $e$.

A semigroup $(S, \cdot)$ consists of a set $S$, an associative binary operation $\cdot$. A monoid $(S, \cdot, e)$ consists of a semigroup $(S, \cdot)$ together with an distinguished identity element $e \in S$.

Exercise: Show that the identity in a monoid is unique. In other words, if $(S, \cdot)$ be a semigroup and if $e$ and $e'$ are two identity elements in $S$, then show that $e = e'$.

Let $a$ be an element of a monoid $(S, \cdot, e)$. An element $b \in S$ is called a left inverse of $a$ if $b \cdot a = e$. An element $e \in S$ is called a right inverse of $a$ if $a \cdot e = e$. An element $d \in S$ is called an inverse of $a$ if $d$ is a left and right inverse of $a$.

Exercise: Suppose $a$ is an element in a monoid $S$ that has a left inverse $b$ and a right inverse $c$. Then show that $b = c$ and further show that $b$ is the unique inverse of $a$. 
An element \( a \) in a monoid \( S \) is called an \textbf{element} of \( S \) if \( a \) has a left and right inverse. By the previous exercise, this inverse is unique, so we denote it by \( a^{-1} \). We shall denote the set of all units in a monoid \( S \) by \( S^* \).

A monoid \((G, \cdot, e)\) is called a \textbf{group} if every element of \( G \) is an \textbf{invertible} element or \textbf{unit}. A monoid or a group \( G \) is called \textbf{abelian} or \textbf{commutative} if \( a \cdot b = b \cdot a \) for all \( a, b \in G \).

The binary operation \( \cdot \) in an abelian group \( G \) is sometimes denoted by \( + \) instead of \( \cdot \), and we call it \textbf{addition} instead of \textbf{multiplication}. Also in these cases the identity of \( G \) is denoted by \( 0 \) instead of \( e \), and the additive inverse of \( a \in G \) is denoted by \(-a\).

A \textbf{ring} \((R, +, \cdot, 0, 1)\) consists of a set \( R \) with two binary operations \( + \) and \( \cdot \), called \textbf{addition} and \textbf{multiplication}, and two distinguished elements \( 0 \) and \( 1 \) (\( 0 \neq 1 \)) such that the following three \textbf{axioms} hold:

- \((R, +, 0)\) is an \textbf{abelian group}.
- \((R, \cdot, 1)\) is a \textbf{monoid} (the element \( 1 \) is called the \textbf{multiplicative identity element} of \( R \)).
- We have \( a \cdot (b + c) = a \cdot b + a \cdot c \) and \((b + c) \cdot a = b \cdot a + c \cdot a\) for all \( a, b, c \in R \). (This property is called the \textbf{distributivity law}).

A ring \( R \) is called \textbf{commutative} if \( a \cdot b = b \cdot a \) for all \( a, b \in R \).

An \textbf{element} \( a \in R \) is called an \textbf{invertible} of \( R \) if \( a \) has a \textbf{multiplicative inverse}, that is, there exists an element, denoted \( a^{-1} \in R \), such that \( a \cdot a^{-1} = a^{-1} \cdot a = 0 \). Recall that we denote the set of all units in \( R \) by \( R^* \).
A commutative ring $R$ is called a field if every nonzero element in $R$ is an unit, or in other words $(R, +, \cdot, 1)$ is an abelian group.

A non-commutative ring $R$ is called a skew field if every nonzero element in $R$ is an unit.

Let $R$ be a ring and let $S$ be a subset of $R$. We say that $S$ is a subring of $R$ if $S$ forms a ring in its own right with the same $0$ and $1$ of $R$ and the operations induced from $R$.

Exercise. Let $R$ be a ring and $S$ be a subset of $R$. Show that $S$ is a subring of $R$ if and only if $S$ satisfies the following properties:

1. $0 \in S$, $1 \in S$.
2. If $a \in S$ and $b \in S$, then $a + b \in S$. (i.e. $S$ is closed under addition)
3. If $a \in S$, then $-(a) \in S$. (i.e. $S$ is closed under negation)
4. If $a \in S$ and $b \in S$, then $a \cdot b \in S$. (i.e. $S$ is closed under multiplication)

Exercise. Let $R$ be a ring and $a \in R$. Show that $a \cdot 0 = 0 \cdot a$ and $(-1) \cdot a = -a = a \cdot (-1)$.

8. First Example of Rings.

We give some basic examples of rings and fields. It is easy to verify that these do satisfy the defining properties of a ring or field. These verifications are left as exercise.
First some examples from the world of numbers:

1. Many familiar number systems form rings with the usual operation of addition and multiplication and the usual 0 and 1.
   Some examples are: $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rational numbers), $\mathbb{R}$ (the real numbers), $\mathbb{C}$ (the complex numbers).
   The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are also fields but $\mathbb{Z}$ is not a field.

   Note that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; so the smaller sets are subgroups (or subfields) of the larger ones.

   Below are some more examples of rings and fields of numbers:

   2. (Exercise) Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, show that $R$ is a subring of $\mathbb{R}$.

      (b) Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, show that $F$ is a subfield of $\mathbb{R}$.

3. A complex number $z$ is called algebraic if there exists rational numbers $a_0, a_1, \ldots, a_n$ (for some $n$) such that

   $$z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0.$$  

   A complex number $z$ is called an algebraic integer if there exists integers $a_0, a_1, \ldots, a_n$ (for some $n$) such that

   $$z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0.$$  

   Let $\overline{\mathbb{Q}}$ be the set of all algebraic numbers and let $\mathbb{A}$ be the set of all algebraic integers.

   Fact: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ and $\mathbb{A}$ is a subring of $\overline{\mathbb{Q}}$. 
The proof of the above fact is not obvious. It would take a while before we are prepared to prove it. The field $\mathbb{Q}$ and its subfields, the ring $\mathbb{A}$ and many of its subrings are basic objects of study in algebraic number theory, so these are important examples of rings and fields.

4. Integers modulo $n$: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, 0, 1)$ form a ring.

For the examples that follow, we fix a commutative ring $R$.

5. A polynomial in one variable $x$ with coefficients in $R$ of degree $n$ is a formal expression of the form $f = a_n x^n + \cdots + a_1 x + a_0$ where $a_0, \ldots, a_n \in R$. The polynomials of degree zero are called constant polynomials. Let $R[x]$ denote the set of all polynomials in one variable $x$ with coefficients in $R$. Then $R[x]$ forms a ring with the usual rules of addition and multiplication of polynomials. The constant polynomials 0 and 1 are the zero and identity in this ring.

A polynomial in two variables $x_1$ and $x_2$ with coefficients in $R$ is a formal expression of the form $f = \sum_{i,j} a_{i,j} x_1^i x_2^j$ where $a_{i,j} \in R$. These can also be added and multiplied by usual rules of polynomial addition and multiplication. Let $R[x_1, x_2]$ denote the set of all polynomials in two variables $x_1$ and $x_2$ with coefficients in $R$. Then $R[x_1, x_2]$ forms a ring. More generally, we have the ring $R[x_1, \ldots, x_n]$ of polynomials in $n$ variables $x_1, \ldots, x_n$ with coefficients in $R$. 

6. **Rings of functions.** Let \( X \) be a set and let \( R \) be a commutative ring. Let \( S \) be the set of all functions from \( X \) to \( R \).

We define the binary operations \( + \) and \( \cdot \) on \( S \) as follows:

If \( f, g \in S \), then define \( (f + g) \) and \( (f \cdot g) \) by

\[
(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (f \cdot g)(x) = f(x) \cdot g(x) \quad \text{for each} \quad x \in X.
\]

Define \( 0 \) and \( 1 \in S \) by \( 0(x) = 0 \) and \( 1(x) = 1 \) for all \( x \in X \).

Then \( (S, +, \cdot, 0, 1) \) is a commutative ring.

We shall write \( S = \text{Fun}(X, R) \).

Many important examples of commutative rings are obtained by considering \( \text{Fun}(X, R) \) and its subrings for various choices of \( X \) and \( R \).

For example, \( C([0, 1]) = \) set of all continuous real-valued functions on \([0, 1]\)
and \( C^\infty([0, 1]) = \) set of all infinitely differentiable real-valued functions on \([0, 1]\)
are two important subrings of \( \text{Fun}([0, 1], IR) \).

Also note that each polynomial \( f(x) \) in one variable \( x \) with real coefficients defines a function from \( IR \) to \( IR \) and the coefficients of this function are determined by this function. Thus \( IR[x] \) can be thought of as a subring of \( \text{Fun}(IR, IR) \). By similar reasoning, \( IR[x_1, \ldots, x_n] \) can be thought of as a subring of \( \text{Fun}(IR^n, IR) \) and \( C[x_1, \ldots, x_n] \) can be thought of as a subring of \( \text{Fun}(C^n, C) \).

7. **Rings of matrices.** Let \( R \) be a commutative ring. Let \( \text{Mat}_n(R) \) denote the set of \( n \times n \) matrices with entries from \( R \). Then \( \text{Mat}_n(R) \) is a ring with respect to matrix addition and matrix multiplication with the identity matrix playing the role of multiplicative identity and the zero matrix playing the role of zero.

For \( n > 1 \), the ring \( \text{Mat}_n(R) \) is non-commutative.
8. Rings of endomorphisms.

Let $M$ be an abelian group. A group homomorphism from $M$ to $M$ is called an endomorphism of $M$. Let $\text{End}(M)$ denote the set of all endomorphisms of $M$. Define two binary operations $+$ and $\circ$ on $\text{End}(M)$ as follows:

Given $f, g \in \text{End}(M)$, define $(f + g)$ and $(f \circ g)$ in $\text{End}(M)$ by:

$(f + g)(m) = f(m) + g(m)$ and $(f \circ g)(m) = f(g(m))$.

Define $0$ and $1$ in $\text{End}(M)$ by $0(m) = 0$ for all $m \in M$ and $1(m) = m$ for all $m \in M$ (so $1$ is the identity function).

Then $(\text{End}(M), +, 0, \circ, 1)$ is a ring.

Many important examples of non-commutative rings arise by considering $\text{End}(M)$ or its subrings for various choices of $M$. 
E. Ring homomorphisms, and ideals.

Let \( R \) and \( S \) be two rings. A ring homomorphism \( f: R \to S \) is a function, \( f \), from \( R \) to \( S \) such that
\[
\begin{align*}
    f(x+y) &= f(x) + f(y) \\
    f(xy) &= f(x)f(y) \\
    f(1) &= 1
\end{align*}
\]

Let \( f: R \to S \) be a ring homomorphism. Define the kernel of \( f \), denoted \( \ker(f) \), by
\[
\ker(f) = \{ x \in R : f(x) = 0 \}.
\]
One easily verifies that \( \ker(f) \) is one to one if and only if \( \ker(f) = \{ 0 \} \).

Exercise: Show that \( \ker(f) \) is an additive subgroup of \( R \).

Show that if \( x, y \in \ker(f) \) then \( xy \in \ker(f) \) and \( x + y \in \ker(f) \).

Definition: Let \( R \) be a ring. A subset \( I \) of \( R \) is called a left ideal of \( R \) if the following conditions hold:
1. \( I \) is an additive subgroup of \( R \).
2. If \( r \in R \) and \( x \in I \), then \( rx \in I \).
3. If \( r \in R \) and \( x \in I \), then \( x \in I \).

Similarly, we define a right ideal \( I \) of \( R \) if the condition (ii) is replaced by the condition (iii). A two sided ideal in \( R \) is a subset that is both a left and a right ideal.

Of course, in a commutative ring every left ideal is also a right ideal and vice versa; we simply call them ideals.

The subset \( \{0\} \) is always an ideal in \( R \). Also \( R \) itself is an ideal in \( R \). These are called the trivial ideals of \( R \).

There are called the non-trivial ideals of \( R \).

By a proper ideal in \( R \) we mean an ideal \( I \) such that \( I \neq R \).

Remark: The exercise above shows that if \( f: R \to S \) is a ring homomorphism then \( \ker(f) \) is a two sided ideal in \( R \).
8. Ideal generated by a subset.

Because: let \( R \) be a ring, let \( \{I_t : t \in T\} \) be a family of left ideals in \( R \). Then verify that \( \bigcap_{t \in T} I_t \) is also a left ideal of \( R \).

The same result holds for right ideals and two-sided ideals.

Definition. Let \( R \) be a ring, let \( A \) be a nonempty subset of \( R \). Let \( I \) be the intersection of all the left ideals of \( R \) that contain \( A \). The above exercise shows that \( I \) itself is a left ideal so \( I \) is the smallest left ideal of \( R \) that contains the subset \( A \).

We say that \( I \) is the left ideal of \( R \) generated by \( A \) and we write \( I = RA \).

Because: show that the left ideal \( RA \) generated by \( A \) consists of all the elements of \( R \) that can be written in the form \( r_1 a_1 + \cdots + r_n a_n \) for some \( r_1, \ldots, r_n \in R \) and \( a_1, \ldots, a_n \in A \) and some \( n \geq 1 \).

The right ideal and two-sided ideal generated by a subset \( A \subset R \) can be defined in similar manners. Of course, if \( R \) is commutative we simply talk of the ideal generated by a subset \( A \).

When \( R \) is a commutative ring and \( A = \{a_1, \ldots, a_n\} \) is a finite subset of \( R \), then the ideal \( RA \) generated by \( A \) is sometimes denoted by \( (Ra_1 + \cdots + Ra_n) \) or sometimes simply denoted by \( (a_1, \ldots, a_n) \).
8. Examples of ideals and ring homomorphisms

1. There is a natural ring homomorphism \( \pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \)
given by \( \pi(k) = \text{mod } n \). The kernel of this homomorphism is
   \[ n\mathbb{Z} = \{ nk : k \in \mathbb{Z} \} \]
   so \( n\mathbb{Z} \) is an ideal in \( \mathbb{Z} \) for each \( n = 0, 1, 2, \ldots \). We know that any additive
   subgroup of \( \mathbb{Z} \) that is not the entire \( \mathbb{Z} \) itself must be of the form \( n\mathbb{Z} \) for some \( n = 1, 2, \ldots \).
   Since every ideal in \( \mathbb{Z} \) is in particular an additive subgroup, it follows
   that the ideals in \( \mathbb{Z} \) are precisely \( n\mathbb{Z} \), \( n = 0, 1, 2, \ldots \).

2. Let \( X \) be any set and \( A \) be any commutative ring.
   Recall that \( \text{Fun}(X, A) \) denotes the set of functions from \( X \) to \( A \).
   We know that \( \text{Fun}(X, A) \) is a commutative ring under pointwise
   addition and multiplication of functions.

   Given any \( x \in X \), define the function \( \text{ev}_x : \text{Fun}(X, A) \to A \)
   by \( \text{ev}_x(f) = f(x) \), for \( f \in \text{Fun}(X, A) \).
   Verify that \( \text{ev}_x \) is a homomorphism from \( X \) to \( A \). These are
   important homomorphisms, called evaluation homomorphisms.

   Notice that the ideal \( \ker(\text{ev}_x) \) in \( \text{Fun}(X, A) \) consists of all \( f \in \text{Fun}(X, A) \) such that \( f(x) = 0 \) for all \( x \).
   \( \ker(\text{ev}_x) = \{ f \in \text{Fun}(X, A) : f(x) = 0 \} \).
In the previous example we saw $f \in \text{Fun}(\mathbb{R}, \mathbb{R})$ is an ideal in $\text{Fun}(\mathbb{R}, \mathbb{R})$. More general examples of similar kind are obtained as follows:

Let $S$ be a subring of $\text{Fun}(\mathbb{R}, \mathbb{R})$, and let $C$ be any subset of $X$. Define

$$I(C) = \{ f \in S : f(c) = 0 \text{ for all } c \in C \}.$$

In other words, $I(C)$ is the set of functions in $S$ that vanish on $C$.

Exercise: Verify that $I(C)$ is an ideal in $S$.

4. Here is a particular illustration of the type of ideals defined in the previous example.

Let $S = \mathbb{R}[x, y]$ be the ring of polynomials in two variables $x$ and $y$ with real coefficients. Note that $S$ can be thought of as a subring of $\text{Fun}(\mathbb{R}^2, \mathbb{R})$.

Let $C = \{(x, y) \in \mathbb{R}^2 : y - x^2 = 0\}$. (a curve in the plane).

Then

$$I(Y) = \{ f \in \mathbb{R}[x, y] : f(c) = 0 \text{ for all } c \in C \}.$$

Since $C = \{(x, x^2) : x \in \mathbb{R}\}$, we find

$$I(Y) = \{ f \in \mathbb{R}[x, y] : f(x, x^2) = 0 \}.$$

One can show that $I(Y) = (y - x^2)S$, but this is not immediate.
5. Here is an example in the world of noncommutative rings.

Let $M_1$ and $M_2$ be two abelian groups and let $M = M_1 \oplus M_2$. Recall that the elements of $M$ are of the form $(m_1, m_2)$ with $m_1 \in M_1$ and $m_2 \in M_2$. The addition on $M$ is defined componentwise.

Consider the ring $\text{End}(M)$ of abelian group homomorphisms from $M$ to $M$. Define

$$I = \{ f \in \text{End}(M) : f(m, 0) = (0, 0) \text{ for all } m \in M_1 \}.$$

Exercise: 9 Verify that $I$ is a left ideal in $\text{End}(M)$.

b) Consider the example $M_1 = M_2 = \mathbb{Z}$, so $M = \mathbb{Z}^2$ (think column vectors of length 2).

We saw in homework that $\text{End}(M)$ can be identified with the ring of $2 \times 2$ integer matrices. Describe the ideal $I$ explicitly in this example.

After we identify $\text{End}(M)$ with the ring of $2 \times 2$ matrices,

9 Verify that in the example $M = \mathbb{Z}^2$, the subset $I$ is a left ideal, but not a right ideal.

Exercises: Can you describe all the left ideals in $\text{End}(\mathbb{Z})$ and all the right ideals in $\text{End}(\mathbb{Z})$.
Let R be a ring and I be a two sided ideal in R. In particular I is a subgroup of the additive group \((R, +)\) so we can consider the quotient additive group \(R/I\).

Recall that the elements of \(R/I\) are the cosets of \(I\) in \(R\), that have the form \(r + I = \{ r + x : x \in I \}\), for some \(r \in R\), and the addition in \(R/I\) is defined such that

\[(r + I) + (s + I) = (r + s) + I.\]

Since I is an ideal in \(R\), one can actually define a second binary operation \((\cdot)\) (multiplication) on \(R/I\) such that \(R/I\) becomes a ring.

The multiplication in \(R/I\) is defined as follows:

Let \((r + I)\) and \((s + I)\) be two elements of \(R/I\). Then we define

\[(r + I) \cdot (s + I) = (rs + I).\]  \((*)\)

Of course we have to verify that this gives a well defined binary operation on \(R/I\). More precisely we have to verify that the coset on the right hand side of \((*)\) only depends on the cosets \((r + I)\) and \((s + I)\) and does not depend on the choice of the particular elements \(r\) and \(s\) from those cosets. Here is the verification:

Let \(r', s' \in R\) be such that \((r' + I) = (r + I)\) and \((s' + I) = (s + I)\). Then \(r' = r + x\) and \(s' = s + y\) with \(x, y \in I\). So

\[r's' = (r + x)(s + y) = rs + x + ys + xy.\]

Since I is a two sided ideal and \(x, y \in I\), we find that \(xs + y + I\) is \(I\). So

\[r's' + I = rs + I.\]

This verifies that \((*)\) is indeed a well defined binary operation on \(R/I\).
It is easy to verify that \( R/I \) becomes a ring with the binary operations \( + \) and \( \cdot \) defined above and with \( 0_{R/I} = 0_R + I \) and \( 1_{R/I} = 1_R + I \).

Recall that we have a natural onto map \( \pi : R \to R/I \) given by \( \pi(r) = r + I \) and that \( \pi \) is an abelian group homomorphism for the additive structure of \( R \) and \( R/I \). From the definition of the multiplication in \( R/I \) (equation (1)), it follows that \( \pi \) is actually an onto ring homomorphism.

The ring \( R/I \) is called the quotient of \( R \) by \( I \) and \( \pi \) is called the natural homomorphism from \( R \) to \( R/I \).

**Example of quotient ring**

1. Consider the quotient \( R[x]/(x^2) \) where \((x^2)\) denotes the ideal generated by \( x^2 \). Explicitly, \((x^2) = \{ \sum f(x) : f \in R[x] \} \) consists of all polynomials of the form \((a_0 x^0 + a_1 x^1 + \ldots + a_n x^n)\) for some \( n \geq 2 \) and \( a_i \in R \).

Let \( \pi : R[x] \to R[x]/(x^2) \) denote the natural projection and let \( \pi \equiv \pi \). Let \( \pi = \pi(x) \).

Show that for any element \( q \in R[x]/(x^2) \) we can write it in the form \( q = a + r, \) where \( a, r \in R \), are uniquely determined by \( q \), so \( R[x]/(x^2) \) is an additive group \( R[x]/(x^2) = (R + R[x]) / \text{isomorphism} \). For \( a \in R \)

Verify that the multiplication in \( R[x]/(x^2) \) is given by

\[
(a + r)(b + s) = (a b + r s) + \text{term involving } x^2.
\]

In other words, the multiplication rule in \( R[x]/(x^2) \) is determined by the multiplication in \( R \) and the rule \( x^2 = 0 \).

We can say that \( R[x]/(x^2) \) is obtained from \( R \) by formally adding a quadratic infinitesimal \( x \) and the natural map \( \pi : R[x] \to R[x]/(x^2) \) corresponds to taking the 1st order Taylor expansion of a function in \( R[x] \).
3. Ring isomorphism theorems

In this section, unless otherwise stated, homomorphism always means ring homomorphism.

3.1. Theorem. Let $A, B, C$ be three ring and let $f : A \to B$ and $g : A \to C$ be two homomorphisms.

(i) if there exists a homomorphism $h : B \to C$ such that $h \circ f = g$, then $\ker(f) \subset \ker(g)$.
(ii) Suppose $f$ is onto and $\ker(f) \subset \ker(g)$.
(a) Then there exists a unique homomorphism $h : B \to C$ such that $h \circ f = g$.
(b) If $g$ is onto, then so is $h$.
(c) If $\ker(g) = \ker(f)$, then $h$ is one to one.
(d) If $g$ is onto and $\ker(g) = \ker(f)$, then $h$ is an isomorphism.

Proof. (i) Exercise.

(ii) (a) Uniqueness: Suppose $h, h'$ be two homomorphisms such that $h \circ f = g = h' \circ f$. Pick $b \in B$. Since $f$ is onto there exists $a \in A$ such that $f(a) = b$. Then $h(b) = h(f(a)) = g(a) = h'(f(a)) = h'(b)$. Thus there can be at most one $h$ with the given properties.

Existence: Let $b \in B$. Suppose $a, a' \in A$ such that $f(a) = f(a') = b$. Then $f(a-a') = 0$, so $(a-a') \in \ker(f)$, so $(a-a') \in \ker(g)$, so $g(a-a') = 0$, so $g(a) = g(a')$. Thus we observe that $g$ takes the same value on all the elements of $A$ that map to $b$. Given $b \in B$, we can pick $a \in A$ such that $f(a) = b$ (since $f$ is onto) and then define $h(b) = g(a)$. Because of our observation, this procedure gives us a well defined function $h : B \to C$. Verify that $h$ is a ring homomorphism. Now suppose $a \in A$. Let $b = f(a)$. So $a$ is an element of $A$ such that $f(a) = b$. So $h(b) = g(a)$, or $h(f(a)) = g(a)$. So $h \circ f = g$. This proves part (a).

(b) Now suppose $g$ is onto. Let $c \in C$. Then there exists $a \in A$ such that $g(a) = c$. It follows that $h(f(a)) = c$, so $h$ is onto. This proves part (b).

(c) Now suppose $g$ is onto and $\ker(f) = \ker(g)$. To show $h$ is one to one, it is enough to verify that $\ker(h) = e_B$. Let $b \in \ker(h)$, that is, $h(b) = e_C$. Pick $a \in A$ such that $f(a) = b$. Then $g(a) = h(f(a)) = h(b) = e_C$, so $a \in \ker(g) = \ker(f)$, so $b = f(a) = e_B$. So $\ker(h) = e_B$. This proves part (c). Part (d) follows from part (b) and (c).

3.2. Corollary. Let $m, n$ be positive integers. Then there exists a unique homomorphism $h : \mathbb{Z}_{mn} \to \mathbb{Z}_m$ such that $h(1 \mod mn) = 1 \mod m$.

Sketch of proof. Let $f : \mathbb{Z} \to \mathbb{Z}_{mn}$ and $g : \mathbb{Z} \to \mathbb{Z}_m$ be the homomorphisms $f(k) = k \mod mn$ and $g(k) = k \mod m$. Then $\ker(f) = mn\mathbb{Z} \subseteq m\mathbb{Z} = \ker(g)$. Now apply the above theorem.

It is convenient to represent the statement of theorem 3.1 in a diagrammatic language. Let us denote an onto homomorphism $f : A \to B$ by a double headed arrow $f : A \Rightarrow B$. The theorem 3.1 says that given

$$
\begin{array}{ccc}
A & \xrightarrow{g} & C \\
\downarrow{f} & & \downarrow{6} \\
B & & \\
\end{array}
$$
with \( \ker(f) \subseteq \ker(g) \), there exists a unique \( h : B \to C \) such that the following diagram commutes:

\[
\begin{array}{ccc}
A & \xrightarrow{g} & C \\
\downarrow{f} & & \downarrow{h} \\
B & \xrightarrow{h} & C \\
\end{array}
\]  

(1)

Saying that the diagram in (1) commutes is a pictorial way of saying that \( g = h \circ f \).

3.3. **Theorem** (The first isomorphism theorem). Let \( \psi : R \to S \) be a ring homomorphism. Let \( I = \ker(\psi) \). Let \( \phi : R \to R/I \) be the natural quotient homomorphism: \( \phi(r) = r + I \). Then there is a unique isomorphism \( \eta : R/I \to \psi(R) \) such that \( \psi = \eta \circ \phi \).

**Proof.** Recall that kernels of homomorphisms are ideals, so \( I \) is an ideal in \( R \). From given data, we get the following diagram of homomorphisms:

\[
\begin{array}{ccc}
R & \xrightarrow{\psi} & \psi(R) \\
\downarrow{\phi} & & \downarrow{\eta} \\
R/I & & \\
\end{array}
\]

Note that the horizontal arrow is simply the given map \( \psi \), but we consider it as a map to the subring \( \psi(R) \) of \( S \). So \( \psi : R \to \psi(R) \) is an onto homomorphism. From the definition of the quotient map, we have \( \ker(\phi) = I = \ker(\psi) \). So by theorem 3.1(d), we get an isomorphism \( \eta : R/I \to \psi(R) \), such that the following diagram commutes:

\[
\begin{array}{ccc}
R & \xrightarrow{\psi} & \psi(R) \\
\downarrow{\phi} & & \downarrow{\eta} \\
R/I & \xrightarrow{\approx} & \\
\end{array}
\]

Saying that the above diagram commutes is just a pictorial way of saying \( \psi = \eta \circ \phi \).  

Let \( R \) be a ring and \( I \) be an ideal. The quotient homomorphism \( R \to R/I \) collapses the ideal \( I \) to the zero ideal in \( R/I \). In this way, considering the quotient group \( R/I \) lets us forget the structure inside \( I \). The correspondence theorem below says that "taking quotient by \( I \) retains the ideal and subring structure in \( R \) above \( I \)". So passing to the quotient group \( R/I \) lets us disregard what was happening inside \( I \) and focus solely on what happens "above" \( I \). In this way, the quotient construction becomes an important simplifying tool.

3.4. **Theorem** (the correspondence theorem). Let \( I \) be an ideal of \( R \). Then

(a) there is a natural inclusion preserving bijection between

\[
\{ \text{set of ideals of } R \text{ containing } I \} \to \{ \text{set of ideals of } R/I \}
\]

Under this bijection, an ideal \( J \) of \( R \) such that \( J \supseteq I \) corresponds to the ideal \( J/I \) of \( R/I \).

(b) There is a natural inclusion preserving bijection between

\[
\{ \text{set of subrings of } R \text{ containing } I \} \to \{ \text{set of subrings of } R/I \}
\]

Under this bijection, a subring \( S \) of \( R \) such that \( S \supseteq I \) corresponds to the ideal \( S/I \) of \( R/I \).

The proof of the correspondence theorem is left as a routine exercise.
3.5. **Theorem** (The second isomorphism theorem). Let $R$ be a ring. Let $J$ be an ideal of $R$. Let $S$ be a subring of $R$. Then $(S + J)$ is a subring of $R$ and $S \cap J$ is an ideal of $S$ and and $S/S \cap J \simeq (S + J)/J$.

**sketch of proof.** Since $(S + J)$ is clearly an additive subgroup of $R$ and it contains $1 = (1 + 0)$, to check $(S + J)$ is a subring of $R$ we only need to verify that $(S + J)$ is closed under multiplication. Let $u_1$ and $u_2$ be two elements of $(S + J)$. Then we can write $u_1 = s_1 + x_1$ and $u_2 = s_2 + x_2$ for some $s_1, s_2 \in S$ and $x_1, x_2 \in J$. Then $u_1u_2 = s_1s_2 + s_1x_2 + x_2s_1 + x_1x_2$. Notice that $s_1s_2 \in S$ since $S$ is a subring and $s_1x_2 + s_2x_1 + x_1x_2 \in J$ since $J$ is an ideal. So $u_1u_2 \in (S + J)$, that is $(S + J)$ is closed under multiplication.

Verifying $S \cap J$ is an ideal of $S$ is left as a routine exercise. Now let $\psi$ be the composition of homomorphisms:

$$S \xrightarrow{\text{inclusion}} (S + J) \xrightarrow{\text{quotient map}} (S + J)/J.$$

So $\psi : S \rightarrow (S + J)/J$ is given by $\psi(s) = s + J$. Note that $\psi$ is a homomorphism since both the inclusion and the quotient map are homomorphisms. Verify that $\psi$ is onto and $\ker(\psi) = S \cap J$. Then the second isomorphism theorem follows from the first isomorphism theorem.

3.6. **Theorem** (The third isomorphism theorem). Let $I$ and $J$ be ideals in a ring $R$ with $J \subset I \subset R$. From the correspondence theorem, we know that $I/J$ is an ideal in $R/J$. There is a natural isomorphism $\frac{R/I}{J} \simeq \frac{R}{I}$.

**sketch of proof.** Consider the following diagram of homomorphisms:

$$\begin{array}{ccc}
R & \xrightarrow{\phi_I} & R/I \\
\downarrow{\phi_J} & & \downarrow{\psi} \\
R/J & & \\
\end{array}$$

where the maps $\phi_I$ and $\phi_J$ are the natural quotient homomorphisms. Note that $\ker(\phi_J) = J \subset I = \ker(\phi_I)$. So by theorem 3.1(c), we have a onto homomorphism $\psi : R/J \rightarrow R/I$ such that the following diagram commutes:

$$\begin{array}{ccc}
R & \xrightarrow{\phi_I} & R/I \\
\downarrow{\phi_J} & & \downarrow{\psi} \\
R/J & & \\
\end{array}$$

If $r \in R$, then one has $\psi(r + J) = \psi \circ \phi_J(r) = \phi_I(r) = r + I$. Now verify that $\ker(\psi) = I/J$ and apply the first isomorphism theorem.

As an application of the isomorphism theorems, we shall prove the Chinese remainder theorem. For this, first we need a little bit about product rings. Let $R_1$ and $R_2$ be two rings. Then the cartesian product $R_1 \times R_2$ becomes a ring with componentwise addition and multiplication: $(r_1, r_2) + (r'_1, r'_2) = (r_1 + r'_1, r_2 + r'_2)$ and $(r_1, r_2). (r'_1, r'_2) = (r_1r'_1, r_2r'_2)$ for $r_1, r'_1 \in R_1$, $r_2, r'_2 \in R_2$ and with $0_{R_1 \times R_2} = (0_{R_1}, 0_{R_2})$, $1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$; this ring is called the product ring of $R_1$ and $R_2$. The product of $n$ rings $R_1, \ldots, R_n$, denoted by $R_1 \times \cdots \times R_n$ is defined similarly. Sometimes we use the abbreviated notation $R_1 \times \cdots \times R_n = \prod_{i=1}^n R_i.$
The product ring comes with natural projection maps \( \pi_j : R_1 \times \cdots \times R_n \to R_j \) given by \( \pi_j(r_1, \ldots, r_n) = r_j \). It is easy to verify that \( \pi_1, \ldots, \pi_n \) are onto ring homomorphisms. The next theorem tells us how to construct homomorphism to a product.

3.7. **Theorem.** Let \( R_1, \ldots, R_n, R \) be rings. Given ring homomorphisms \( f_j : R \to R_j \) for \( j = 1, \ldots, n \), there exists a unique homomorphism \( f : R \to \prod_{j=1}^n R_j \) such that \( \pi_j \circ f = f_j \) for \( j = 1, \ldots, n \). (where \( \pi_j : R_1 \times \cdots \times R_n \to R_j \) denotes the natural projections). We shall write \( f = (f_1, \ldots, f_n) \).

**Sketch of proof.** Define \( f : R \to \prod_{j=1}^n R_j \) by \( f(r) = (f_1(r), \ldots, f_n(r)) \) and verify that \( f \) is a homomorphism and that \( \pi_j \circ f = f_j \) for each \( j \). The uniqueness of \( f \) is easy to verify as well.

3.8. **Theorem.** Let \( R \) be a commutative ring. Let \( M_1, \ldots, M_n \) be two ideals in \( R \) and let \( M = M_1 \cap \cdots \cap M_n \). Let \( \pi_j : R \to R/M_j \) be the natural quotient homomorphisms for \( j = 1, \ldots, n \). Let \( f = (\pi_1, \ldots, \pi_n) : R \to (R/M_1 \times \cdots \times R/M_n) \) and let \( \pi : R \to R/M \) be the quotient homomorphism. Then there exists an unique injective homomorphism \( \alpha : R/M \to R/M_1 \times \cdots \times R/M_n \) such that \( \alpha \circ \pi = f \).

**Sketch of proof.** The previous lemma yields the map \( f : R \to \prod_{j=1}^n R/M_j \) given by \( f(r) = (r+M_1, \ldots, r+M_n) \). Verify that \( \ker(f) = M_1 \cap \cdots \cap M_n = M \) and apply the first isomorphism theorem.

3.9. **Definition.** Let \( I, J \) be ideals in a commutative ring \( R \). We let \( IJ \) denote the ideal generated by the products of the form \( xy \) with \( x \in I \) and \( y \in J \). So \( IJ \) consists of all the elements of the form \( (x_1y_1 + \cdots + x_ny_n) \) where \( x_1, \ldots, x_n \in I \) and \( y_1, \ldots, y_n \in J \) and for some \( n \geq 1 \).

Let \( I + J \) denote all elements of the form \( x + y \) with \( x \in I \) and \( y \in J \). Notice that \( (I + J) \) is the smallest ideal containing \( I \) and \( J \). Two ideals \( I \) and \( J \) in a commutative ring \( R \) are called co-maximal if \( I + J = R \).

3.10. **Lemma.** Let \( M_1, \ldots, M_n \) be ideals in a commutative ring \( R \). Then (a) \( M_1 \cdots M_n \subseteq M_1 \cap \cdots \cap M_n \).

(b) Suppose \( M_1 + M_2 = R \). Then \( M_1 \cap M_2 = M_1M_2 \).

(c) Suppose \( M_i + M_j = R \) for all \( i \neq j \). Then \( M_j + M_1 \cdots M_{j-1}M_{j+1} \cdots M_n = R \) for all \( j \).

(d) Suppose \( M_i + M_j = R \) for all \( i \neq j \). Then \( M_1 \cap \cdots \cap M_n = M_1 \cdots M_n \).

**Proof.** Part (a) is easy to verify. (b) suppose \( M_1 \) and \( M_2 \) are co-maximal. Then there exists \( x \in M_1 \) and \( y \in M_2 \) such that \( (x+y) = 1 \). If \( z \in M_1 \cap M_2 \), then \( z = z(x+y) = zx + zy \). Now note that \( zx \) and \( zy \) are both in \( M_1M_2 \). So \( z = (zx + zy) \in M_1M_2 \) as well. So \( M_1 \cap M_2 \subseteq M_1M_2 \).

(c) We shall argue that \( M_1 \) and \( M_2 \cdots M_n \) are co-maximal. Since \( M_1 + M_j = R \), for each \( j = 2, \ldots, n \), we can find \( a_j \in M_1 \) and \( b_j \in M_j \) such that \( a_j + b_j = 1 \). Then \( b_2 \cdots b_n = (1-a_2) \cdots (1-a_n) = 1 - a \) for some \( a \in M_1 \). So \( a + b_2 \cdots b_n = 1 \), where \( a \in M_1 \) and \( b_2 \cdots b_n \in M_2 \cdots M_n \). This shows \( M_1 \) and \( M_2 \cdots M_n \) are co-maximal. Similarly, we get \( M_j \) and \( M_1 \cdots M_{j-1}M_{j+1} \cdots M_n \) are co-maximal for each \( j \).

(d) We induct on \( n \). Part (b) gives the case \( n = 2 \). By induction, suppose that the result is true for \( n-1 \), so \( M_2 \cdots M_n = M_2 \cap \cdots \cap M_n \). From part (c), we get \( M_1 + M_2 \cdots M_n = R \), so \( M_1 \cap M_2 \cdots M_n = M_1M_2 \cdots M_n \). By induction hypothesis it follows that \( M_1 \cap M_2 \cdots M_n = M_1M_2 \cdots M_n \).
3.11. **Theorem** (Chinese remainder theorem for commutative rings). Let \( M_1, \ldots, M_n \) be ideals in a commutative ring \( R \) and let \( M = M_1 \cap \cdots \cap M_n \). Assume that \( M_i + M_j = (1) \) for all \( i \neq j \). Then \( M = M_1 \cdots M_n \) and \( R/M \cong (R/M_1 \times \cdots \times R/M_n) \).

**Proof.** In 3.10(d) we already saw that the conditions \( M_i + M_j = (1) \) for all \( i \neq j \) imply \( M = M_1 \cdots M_n = M_1 \cap \cdots \cap M_n \). From 3.8 we have an injection
\[
\alpha : R/M \rightarrow R/M_1 \times \cdots \times R/M_n
\]
given by \( \alpha(r + M) = (r + M_1, \ldots, r + M_n) \). We need to verify that \( \alpha \) is onto. For each \( i \), let \( N_i = M_1M_2 \cdots M_{i-1}M_{i+1} \cdots M_n \). From lemma 3.10(c), we know \( M_i + N_i = (1) \), so there exists \( b_i \in M_i \) and \( e_i \in N_i \) such that \( e_i + b_i = 1 \). An element of \( R/M_1 \times \cdots \times R/M_n \) has the form \( (c_1 + M_1, \ldots, c_n + M_n) \), for some \( c_1, \ldots, c_n \in R \). Given this element, take \( c = (c_1 e_1 + \cdots + c_n e_n) \). For each \( k \), note that \( e_k \in N_k \) implies that \( e_k \) belongs to each of the ideals \( M_1, M_2, \ldots, M_{k-1}, M_{k+1}, \ldots, M_n \). So
\[
c \mod M_i = c_i e_i \mod M_i = c_i(1 - b_i) \mod M_i = c_i \mod M_i
\]
since \( b_i \in M_i \). Hence \( \alpha(c + M) = (c_1 + M_1, \ldots, c_n + M_n) \). \( \square \)

3.12. **Corollary.** Let \( m_1, \ldots, m_n \) be nonzero integers and \( m = m_1 \cdots m_n \). If \( \gcd(m_i, m_j) = 1 \) for each pair \( i \neq j \), then \( \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \).

**Proof.** Follows from the previous theorem with \( M_j = m_j \mathbb{Z} \), once we observe that \( m_i, m_j \) relatively prime implies \( M_i + M_j = (1) \) and \( M_1 \cdots M_n = m \mathbb{Z} \). \( \square \)
4. Maximal ideals and prime ideals

4.1. Lemma. A commutative ring $R$ is a field if and only if the only ideal in $R$ is $\{0\}$ and $R$ itself.

**solution.** Suppose $R$ is a field. Let $I$ be a nonzero ideal in $R$. Choose $a \in I$ such that $a \neq 0$. Since $R$ is a field $a$ has a multiplicative inverse in $R$, denoted $a^{-1}$. Since $I$ an ideal $1 = a^{-1}a \in I$. So for any $b \in R$, we have $b = b.1 \in I$, so $R = I$. So the only ideals in $R$ are $\{0\}$ and $R$.

Conversely, suppose the only ideals in $R$ are $\{0\}$ and $R$. Let $a$ be a non-zero element of $R$. Then the ideal $aR$ generated by $a$ contains $a = a.1$, so $aR \neq \{0\}$, so we must have $aR = R$; hence $1 \in aR$. In other words, there exists $b \in R$ such that $ab = 1$. So every nonzero $a \in R$ has a multiplicative inverse in $R$ and hence $R$ is a field. $\square$

A proper ideal $M$ in a ring $R$ is called maximal if $M$ is not a proper subset of any ideal of $R$ except $R$ itself.

4.2. Theorem. Let $R$ be a commutative ring. An ideal $M$ in $R$ is maximal if and only if $R/M$ is a field.

**Proof.** Consider the quotient map $\pi : R \to R/M$. By the correspondence theorem, there is a bijection between the set of ideals of $R$ that contain $M$ and the set of ideals of $R/M$. If $R/M$ is a field, then there are no proper nontrivial ideals in $R/M$, which implies, by the correspondence theorem, that there are no proper ideals in $R$ that strictly contains $M$, that is, $M$ is maximal. Conversely, if $M$ is maximal, then there is no proper ideal of $R$ that strictly contains $M$, so by correspondence theorem, $R/M$ has no proper non-trivial ideal, so $R/M$ is a field. $\square$

4.3. Definition (principal ideals). Let $R$ be a commutative ring and $I$ be an ideal in $R$. Say that $I$ is a principal ideal if $I$ can be generated by a single element of $R$, that is, $I$ has the form $I = aR = \{ar : r \in R\}$ for some $a \in R$. If $I = aR$, the we say that $I$ is the principal ideal generated by $a$, or that $a$ is a generator for the principal ideal $I$. Sometimes we also use the notation $(a) = aR$ to denote a principal ideal. Verify that if $a$ and $a'$ are two generators of the same principal ideal, then $a'$ is an unit multiple of $a$. In other words, the generator of a principal ideal is unique upto units. An integral domain $R$ is called a principal ideal domain or a PID if every ideal in $R$ is principal. We have seen that $\mathbb{Z}$ is a PID.

4.4. Definition (divisibility among ideals, prime ideals). Let $R$ be a commutative ring. Let $a, b \in R$. Say that $a \mid b$ in $R$ if there exists $c \in R$ such that $ac = b$. This is equivalent to $(a) \supseteq (b)$ or $b \in (a)$. In general, if $I$ and $J$ are two ideals in $R$, we say that $I \mid J$ if $I \supseteq J$. If $a \in R$, we say $I \mid a$, if $I \supseteq a$, that is, $a \in I$. An proper ideal $P$ in $R$ is called a prime ideal if $ab \in P$ implies $a \in P$ or $b \in P$. An element $p \in R$ is called a prime element if $(p)$ is a prime ideal. In other words, $p \mid ab$ implies $p \mid a$ or $p \mid b$.

4.5. Example: (a) The prime ideals in $\mathbb{Z}$ are precisely the ideals generated by prime numbers and the ideal $\{0\}$. If $p$ is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is actually a field, so $p\mathbb{Z}$ is actually a maximal ideal. On the other hand, the prime ideal $\{0\}$ is clearly not maximal.

4.6. Lemma. Let $R$ be a commutative ring. Then $P$ is a prime ideal in $R$ if and only if $R/P$ is a domain. Since every field is a domain, it follows that every maximal ideal in $R$ is a prime ideal.
4.7. Lemma. (a) Let $R$ be a commutative domain. Then prime elements in $R$ are irreducible.

(b) Let $R$ be a PID. Then an irreducible in $R$ is a prime element.

Proof. (a) Let $(p)$ be a prime ideal in $R$. If possible suppose $p = uv$. Then $uv \in (p)$, so either $u \in (p)$ or $v \in (p)$. If $u \in (p)$, then $u = cp$, so $cv = 1$, that is $v$ is an unit. Similarly, if $v \in (p)$, then $u$ is an unit.

(b) Let $p \in R$ be irreducible. Suppose $ab \in (p)$. Since $R$ is a PID, the ideal $(a, p)$ has a generator, say $x$, that is, $(x) = (a, p)$. Then $p \in (x)$, so $p = xu$ for some $u \in R$. Since $p$ is irreducible, either $u$ or $x$ must be an unit and we consider these two cases separately: In the first case, when $u$ is an unit, then $x = u^{-1}p$, so $a \in (x) \subseteq (p)$, that is, $p$ divides $a$. In the second case, when $x$ is a unit, then $(a, p) = (1)$. So $(ab, pb) = (b)$. But $(ab, pb) \subseteq (p)$. So $(b) \subseteq (p)$, that is $p$ divides $b$. \qed
5. POLYNOMIAL RINGS

Let \( R \) be a commutative ring. A polynomial of degree \( n \) in an indeterminate (or variable) \( x \) with coefficients in \( R \) is an expression of the form \( f = a_0 + a_1 x + \cdots + a_n x^n \), where \( a_0, \ldots, a_n \in R \) and \( a_n \neq 0 \). We say that \( a_0, \ldots, a_n \) are the coefficients of \( f \) and that \( a_n x^n \) is the highest degree term of \( f \). A polynomial is determined by its coefficients. Two polynomials \( f = \sum_{i=0}^{m} a_i x^i \) and \( g = \sum_{i=1}^{n} b_i x^i \) are equal if \( m = n \) and \( a_i = b_i \) for \( i = 0, 1, \ldots, n \).

Degree of a polynomial is a non-negative integer. The polynomials of degree zero are just the elements of \( R \), these are called constant polynomials, or simply constants. Let \( \mathbb{R} \) denote the set of all polynomials in the variable \( x \). The addition and multiplication of polynomials are defined in the usual manner: If \( f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \) and \( g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n \) are two elements of \( \mathbb{R} \), then their sum is

\[
\sum_{i=0}^{m} a_i x^i + \sum_{i=1}^{n} b_i x^i = \sum_{i=1}^{\max(m,n)} (a_i + b_i) x^i + \sum_{i=\max(m,n)+1}^{\min(m,n)} b_i x^i + \sum_{i=\min(m,n)+1}^{m+n} a_i x^i
\]

and their product is defined by

\[
f(x) \cdot g(x) = \sum_{j=0}^{m+n} \left( \sum_{i=0}^{j} a_i b_{j-i} \right) x^j
\]

Let 1 denote the constant polynomial 1 and 0 denote the constant polynomial zero. Then \( \mathbb{R} \) is a commutative ring. The ring axioms are easily verified.

5.1. Lemma. Let \( R \) be a domain. Then \( \deg(fg) = \deg(f) + \deg(g) \).

Proof. Suppose \( \deg(f) = m \) and \( \deg(g) = n \). Then \( f \) and \( g \) has the form \( f = \sum_{j=0}^{m} a_j x^j \) and \( g = \sum_{k=0}^{n} b_k x^k \) where \( a_m \neq 0 \) and \( b_n \neq 0 \). From the definition of polynomial multiplication, one notices that the highest degree term of \( fg \) is \( a_m b_n x^{m+n} \). Since \( R \) is a domain, \( a_m b_n \neq 0 \), so \( fg \) has degree \( m+n \).

5.2. Corollary. Let \( R \) be a domain.

(a) Then \( \mathbb{R} \) is a domain.

(b) The units in \( \mathbb{R} \) are precisely the constant polynomials that are also units in \( R \).

Proof. (a) Let \( f, g \in \mathbb{R} \) such that \( fg = 0 \). then \( \deg(f) + \deg(g) = \deg(0) = 0 \) (since the zero polynomial is a constant, so it has degree zero). Since degree is a nonzero integer, it follows that \( \deg(f) = 0 \) and \( \deg(g) = 0 \), so \( f \) and \( g \) are constants, i.e, \( f \) and \( g \) are just elements of \( R \). Now, since \( R \) is a domain, it follows that \( f = 0 \) or \( g = 0 \).

(b) Let \( u \) be an unit of \( \mathbb{R} \). Then there exists \( v \in \mathbb{R} \) such that \( uv = 1 \), so \( \deg(u) + \deg(v) = \deg(1) = 0 \), so \( \deg(u) = \deg(v) = 0 \), that is, \( u \) and \( v \) are constants, that is, \( u \) and \( v \) are elements of \( R \). Now \( uv = 1 \) says that \( u \) is an unit of \( R \).

5.3. Definition (evaluation at a point). Let \( f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R} \) be a polynomial and \( r \in R \). Then we let \( f(r) = a_0 + a_1 r + \cdots + a_n r^n \). We say that \( f(r) \) is the value of the polynomial \( f(x) \) at \( r \). We say that \( a \in \mathbb{R} \) is a root of the polynomial \( f \) if \( f(a) = 0 \). This way each polynomial \( f(x) \) determines a function \( f : R \to R \) that takes \( r \in R \) to \( f(r) \). Notice that if \( f = g \), then \( f(r) = g(r) \) for all \( r \in R \). Define a function \( ev_r : \mathbb{R} \to R \) given by \( ev_r(f) = f(r) \). One verifies that \( ev_r \) is a ring homomorphism from \( \mathbb{R} \) to \( R \); it is called the evaluation homomorphism. We also say that \( ev_r(f) = f(r) \) is the element of \( R \) obtained by evaluating \( f \) at \( r \).
For the rest of this section, we let $F$ be a field and we consider polynomial ring in one variable over the field $F$. If $p \in \mathbb{Z}$ is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field with $p$ elements. We write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

5.4. **Theorem** (Euclidean algorithm). Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$.

**Sketch of proof.** Follows from the Euclidean algorithm for division of polynomials. See the book for details. □

5.5. **Example** Examples of polynomial division in $\mathbb{Q}[X]$:

$$(2x^2 - x + 1)(x^3 - \frac{1}{2}x + \frac{1}{2}) + (x + \frac{1}{2}) = 2x^5 - x^4 + \frac{3}{2}x^2 + 1$$

Divide the right hand side by $2x^2 - x + 1$ and check that $(x^3 - \frac{1}{2}x + \frac{1}{2})$ is the quotient and $(x + \frac{1}{2})$ is the remainder.

5.6. **Corollary.** $F[x]$ is a PID.

**Sketch of proof.** Given an ideal $I$ find the polynomial of least degree in $I$ and show that it generates $I$. □

5.7. **Corollary.** Let $F$ be a field. A polynomial $f \in F[x]$ has a root $a \in F$ if and only if $(x - a)$ divides $f$ in $F[x]$.

**Proof.** If $(x - a)$ divides $f$ in $F[x]$, then $f(x) = (x - a)g(x)$ for some $g \in F[x]$, so $f(a) = (a - a)g(a) = 0$, so $a$ is a root of $f$. Conversely, suppose $a$ is a root of $f$. By Euclidean algorithm, we can divide $f$ by $(x - a)$ and write $f(x) = (x - a)g(x) + r$ where $g, r \in F[x]$ and $\deg(r) < \deg(x - a) = 1$, so $\deg(r) = 0$, that is $r \in F$ is a constant. Evaluating both sides at $a$ we obtain $0 = f(a) = (a - a)g(a) + r = r$, so $r = 0$, hence $f(x) = (x - a)g(x)$. □

5.8. **Reducing coefficients modulo an ideal:** Let $\phi : R \to S$ be a ring homomorphism. Then verify that $\phi$ determines a ring homomorphism $\Phi : R[x] \to S[x]$ given by $\Phi(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$. In particular, if $I$ is an ideal in $R$, then we have the natural quotient homomorphism $\pi : R \to R/I$ and hence we have a ring homomorphism $R[x] \to R/I[x]$ obtained by taking a polynomial and reducing its coefficients modulo $I$. This homomorphism takes $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ to $f \mod I$, where $f \mod I$ is defined to be $f \mod I = (a_0 \mod I) + (a_1 \mod I)x + \cdots + (a_n \mod I)x^n$. If $a$ is a root of $f$ in $R$, then reducing coefficients modulo $I$, we find that $a \mod I$ is a root of $f \mod I$. In particular, if $f$ has a root in $R$, then $f \mod I$ has a root in $R/I$.

Recall that an element $f$ is a PID $R$ is called irreducible, if $f = uv$ with $u, v \in R$ implies that either $u$ or $v$ is an unit. An element is called reducible if it is not irreducible. The units in $F[x]$ are just the nonzero constants (since $F$ is a field). Given any $f \in F[x]$ and a constant $u \in F \setminus \{0\}$, we can always write $f = u(u^{-1}f)$; this is called a trivial factorization. So a non-trivial factorization of $f \in F[x]$ is a factorization $f = gh$ where both $g$ and $h$ has degree at least 1. The irreducible polynomials in $F[x]$ are the polynomials that “cannot be non-trivially factored”.

5.9. **Exercise:** (a) Show that $f(x) = x^3 - 3x + 3$ is irreducible in $\mathbb{Q}[x]$.

(b) Show that $f(x) = x^3 - 3x + 3$ is reducible in $\mathbb{F}_5[x]$
**sketch of proof.** Suppose $f$ is reducible. If $f = gh$ is a nontrivial factorization of $f$, then $\deg(g) + \deg(h) = 3$, so either $g$ has degree 1 and $h$ has degree 2 or vice versa (since $g$ and $h$ are not constants). So $f$ has a factor of the form $(ax+b)$ where $a, b \in Q$ and $a \neq 0$. It follows that $-b/a$ is a root of $f$, so $f$ has a root in $Q$. Write the root of $f$ in the form $m/n$ where $m, n \in Z$ with $gcd(m, n) = 1$. Then $f(m/n) = 0$ implies $m^3 - 3mn^2 + n^3 = 0$. So $n$ divides $3mn^2 - n^3 = m^3$ but $gcd(m, n) = 1$, so $n = 1$. It follows that $f$ has an integer root. Now since $f \in Z[x]$, we can reduce coefficients modulo 2 and obtain a polynomial $f \mod 2 \in F_2[x]$. Note that $f \mod 2$ does not have a solution in $F_2$, since $f(0) \equiv 1 \mod 2$ and $f(1) \equiv 1 \mod 2$. It follows that $f$ does not have an integer root, which is a contradiction. So $f$ is irreducible in $Q[x]$. On the other hand, note that $f(2) \equiv 0 \mod 5$. so 2 is a solution of $f$ in $F_5$. Divide $f$ by $(x-2)$ in $F_5[x]$, to find the factorization $f(x) \equiv (x + 1)^2(x - 2) \mod 5$. $\square$
6. PID and UFD

Let $R$ be a commutative ring. Recall that a non-unit $x \in R$ is called irreducible if $x$ cannot be written as a product of two non-unit elements of $R$ i.e. $x = ab$ implies either $a$ is an unit or $b$ is an unit. Also recall that a domain $R$ is called a principal ideal domain or a PID if every ideal in $R$ can be generated by one element, i.e. is principal.

6.1. Lemma. (a) Let $R$ be a commutative domain. Then prime elements in $R$ are irreducible. (b) Let $R$ be a PID. Then an irreducible in $R$ is a prime element.

Proof. (a) Let $(p)$ be a prime ideal in $R$. If possible suppose $p = uv$. Then $uv \in (p)$, so either $u \in (p)$ or $v \in (p)$, if $u \in (p)$, then $u = cp$, so $cv = 1$, that is $v$ is an unit. Similarly, if $v \in (p)$, then $u$ is an unit.

(b) Let $p \in R$ be irreducible. Suppose $ab \in (p)$. Since $R$ is a PID, the ideal $(a, p)$ has a generator, say $x$, that is, $(x) = (a, p)$. Then $p \in (x)$, so $p = xu$ for some $u \in R$. Since $p$ is irreducible, either $u$ or $x$ must be an unit and we consider these two cases separately: In the first case, when $u$ is an unit, then $x = u^{-1}p$, so $a \in (x) \subseteq (p)$, that is, $p$ divides $a$. In the second case, when $x$ is a unit, then $(a, p) = (1)$. So $(ab, pb) = (b)$. But $(ab, pb) \subseteq (p)$. So $(b) \subseteq (p)$, that is $p$ divides $b$.

Because of the above result, we shall not distinguish between prime elements and irreducible elements in a PID.

6.2. Examples of PIDs: Let $k$ be a field. Then we have seen $k[x]$ is a PID. Also $\mathbb{Z}$ is a PID. A little later, we shall prove that $\mathbb{Z}[i]$ and $\mathbb{Z}[e^{2\pi i/3}]$ are examples of PID. We have also seen in homework exercise that $\mathbb{Z}[\sqrt{-5}]$ is not a PID. Also one easily see that $k[x, y]$ is not a PID, since one can prove that the ideal $(x, y)$ cannot be generated by a single element.

6.3. Definition. Let $R$ be a ring and $a_1, \ldots, a_n \in R$. Then the ideal $(a_1, \ldots, a_n)$ has a generator $x$. Verify that $x$ divides each $a_j$ and if $y$ is some element of $R$ that divides each $a_j$, then $y$ divides $x$. So we say that $x$ is the g.c.d. of $a_1, \ldots, a_n$. Since the generator of a principal ideal is unique up to units, the g.c.d of $a_1, \ldots, a_n$ is unique up to units. We say that two elements $a$ and $b$ in a PID are relatively prime, if their g.c.d. is 1.

We repeat that when we say $d$ is the greatest common divisor of $a_1$ and $a_2$, it simply means that $d$ is a generator for the ideal $(a_1, a_2)$, that is, $(d) = dR = (a_1, a_2)$. So the g.c.d $d$ can be written in the form $d = ra_1 + sa_2$ for some $r,s \in R$.

6.4. Definition. A commutative ring $R$ is called Noetherian if given any increasing sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in $R$, there exists a natural number $n$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$. In words, we say that $R$ is Noetherian if any increasing sequence of ideals in $R$ stabilizes.

6.5. Lemma. A PID is Noetherian.

Proof. Let $R$ be a PID. Let $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$ be a increasing sequence of ideals in $R$. Then verify that $I = \cup (a_i)$ is an ideal, so there exists $a \in R$ such that $I = (a)$. There is a $j \geq 1$ such that $a \in (a_j)$. It follows that $(a) = (a_j) = (a_{j+1}) = \cdots$.

6.6. Definition. A domain $R$ is called an unique factorization domain or an UFD if every nonzero element can be written, uniquely up to units as a product of irreducible elements.

6.7. Theorem. Every PID is an UFD.
Proof. Fix a $a \in R$. We want to write $a$ as a product of primes (equivalently irreducibles) and show that such a decomposition is unique up to permutation of the prime factors and up to units.

**Step 1:** Any non-unit $a$ is divisible by an irreducible element. Suppose not. Since $a$ is not irreducible write $a = a_1b_1$ where $a_1, b_1$ are non-units. Since $a_1 \mid a$, $a_1$ is not irreducible, so write $a_1 = a_2b_2$ where $a_1, b_1$ are non-units. Continuing this way we get a strictly increasing infinite sequence of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ which, is not possible by lemma 6.5. This proves step 1.

**Step 2:** Any $a$ is a product of irreducibles and an unit. Suppose not. By step 1, write $a = p_1c_1$ where $p_1$ is an irreducible. Then $c_1$ is not a unit. So write $c_1 = p_2c_2$ where $p_2$ is irreducible. Continuing this way we get a sequence $(c_1) \subset (c_2) \subset (c_3) \subset \cdots$ which, is not possible by lemma 6.5. So This proves step 2.

**Step 3:** By step 2 we can write $a = p_1p_2\cdots p_r$ where $p_i$ are irreducible elements, not necessarily all distinct. Let $a = p_1p_2\cdots p_r = q_1\cdots q_s$ be two such decompositions. Each $q_j$ is a prime and $q_j \mid p_i \cdots p_r$, hence $q_j = q_i$ for some $i$, hence $q_j = u_jp_i$ for some unit $u_j$. Similarly each $p_i$ is equal to some $q_j$ up to a unit. If there are more $p$'s than $q$'s then canceling all the $q$'s will yield a product of $p$'s equal to an unit which is impossible. So $r = s$ and $p_i$ and $q_i$ are same up to units and up to permutation. \hfill \Box

6.8. Remark. The rings $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ are all UFD’s. This in particular proves that every integer can be written uniquely a a product of positive primes and ±1 and that every polynomial in one variable can be written as a product of irreducible polynomials that are unique up to a scalar.

Let $R$ be an UFD and $a \in R$. We can write $a = \prod p_i^{e(p)}$ where the product is over distinct primes of $R$ and almost all $e(p)$ is zero. The numbers $e(p)$ is uniquely determined by $a$ and $p$. In fact $e(p)$ is the largest integer $n$ such that $p^n \mid a$. This is because $a' = a/p^{e(p)}$ is a product over primes different from $p$, so $p \nmid a'$, i.e. $p^{e(p)+1} \nmid a$. We write $e(p) = \text{ord}_p(a)$.

6.9. **Lemma** (Exercise). Let $R$ be a PID and $a, b, c \in R$. Suppose $(a, b) = (1)$ and $a \mid bc$. Then $a \mid c$.

Proof. Since $(a, b) = (1)$, there exists $r, t \in R$ such that $ar + bt = 1$. So $c = acr + bct$. Since $a$ divides both $acr$ and $bct$, it follows that $a$ divides $c$. \hfill \Box

6.10. **Exercise** Let $I, J$ be two ideals in a commutative ring $R$. Let $x_1, \ldots, x_m$ be a set of generators for $I$ and let $y_1, \ldots, y_n$ be a set of generators for $J$. Then show that \{ $x_iy_j: i = 1, \ldots, m, j = 1, \ldots, n$ \} is a set of generators for the ideal $IJ$.

6.11. **Exercise:** Let $R = \mathbb{Z}[[\sqrt{-5}]] = \{ a + b\sqrt{-5}: a, b \in \mathbb{Z} \}$.

(a) Let $I = (2, 1 + \sqrt{-5})$ (recall that this denotes the ideal in $R$ generated by 2 and $(1 + \sqrt{-5})$). Let $J = (2, 1 - \sqrt{-5})$. Show that $I = J$. Show that $2R = IJ = I^2$.

(b) Show that $R/I \simeq \mathbb{Z}/2\mathbb{Z}$ and conclude that $I$ is a maximal ideal in $R$, hence a prime ideal.

(c) Show that $I$ is not a principal ideal. (Hint: Let $u, v \in R$. Observe that if $u$ divides $v$ in $R$, then $|u|^2$ divides $|v|^2$ in $\mathbb{Z}$).

17
Proof. (a) Show that \(2 \in I\) and \(1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in I\), so \(J \subseteq I\). Again, \(2 \in J\) and \((1 + \sqrt{5}) = 2 - (1 - \sqrt{-5}) \in J\), so \(I \subseteq J\). By the previous exercise, we know \(IJ = \langle 2 \rangle \). Verify that the only commutative ring of size 2 is \(\mathbb{Z}/2\mathbb{Z}\). So \(I \subseteq J\). On the other hand \(2 = 6 - 4 \in IJ, \) so \(2IJ \subseteq IJ\). It follows that \(I^2 = IJ = 2R\).

(b) If \(R = I\), then we would have \(1 = 1.1 \in I^2\), which would imply \(R = I^2 = 2R\), but then \(1 = 2x\) for some \(x \in R\), which would imply \(1/2 \in R\) which is not true. So \(R \neq I\). Also note that \((1 + \sqrt{-5}) \in I \setminus I^2\), since \((1 + \sqrt{-5})/2 \notin R\). So \(I\) is a proper ideal in \(R\) and \(I^2\) is a proper subset of \(I\). Now \(R/I^2 = R/2R\). Verify that \(R/2R = \{0 + 2R, 1 + 2R, \sqrt{-5} + 2R, 1 + \sqrt{-5} + 2R\}\) and these four cosets are distinct, so \(|R/2R| = 4\).

By the third isomorphism theorem, we have \(R/I \simeq R/I^2\). Since \(I \neq I^2\), we have \(|I/I^2| > 1\), so \(|R/I|\) is a proper factor of 4, so \(|R/I| = 1\) or 2. Finally \(R \neq I\) implies \(|R/I| \neq 1\), so \(R/I\) has size 2. Verify that the only commutative ring of size 2 is \(\mathbb{Z}/2\mathbb{Z}\). So \(R/I \simeq \mathbb{Z}/2\mathbb{Z}\).

(c) If \(z = (\alpha + i\beta) \in R\), we write \(|z|^2 = z\bar{z} = \alpha^2 + \beta^2\) and call it the norm of \(z\). Note that the norm of every element of \(R\) is an integer. Suppose \(u\) divides \(v\) in \(R\). Then \(u = vx\) for some \(x \in R\). So \(\bar{u} = \bar{v}\bar{x}\), hence \(\bar{u}u = \bar{v}\bar{x}x\) or \(|u|^2 = |v|^2|x|^2\). Since \(|x|^2\) is an integer, it follows that the integer \(|u|^2\) must divide the integer \(|v|^2|\). If possible, suppose \(I = aR\) for some \(a \in R\). Then \(a\) divides both \((1 + \sqrt{-5})\) and \(2\) in \(R\). So \(|a|^2\) divides \(|1 + \sqrt{-5}|^2 = 6\) and \(|2|^2 = 4\). So \(|a|^2\) divides 2. So \(|a|^2 = 1\) or 2. Write \(a = m + \sqrt{-5}n\) with \(m, n \in \mathbb{Z}\). Then \(m^2 + 5n^2 = |a|^2\). This forces \(m = \pm 1\) and \(n = 0\), and hence \(a = \pm 1 \in R\) and thus \(R = I\) which we have already seen to be false. This contradiction shows that \(I\) is not principal. \(\square\)

6.12. Definition. A domain \(R\) is called an Euclidean domain if there exists a function \(\nu : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}\) such that given any \(a, b \in R\) with \(b \neq 0\), there exists \(q, r \in R\) such that \(a = bq + r\) and \(\nu(r) < \nu(b)\) or \(r = 0\). We say that \(\nu(b)\) is the Euclidean valuation of \(b\).

6.13. Lemma. (i) The ring of integers \(\mathbb{Z}\) is an Euclidean domain with \(\nu(n) = |n|\).

(ii) Let \(k\) be a field. The polynomial ring \(k[x]\) is an Euclidean domain with \(\nu(f) = \deg(f)\).

(iii) The ring \(\mathbb{Z}[i]\) is an Euclidean domain with \(\nu(z) = |z|^2\).

Proof. We already know parts (i) and (ii) from the Euclidean division algorithm in \(\mathbb{Z}\) and \(k[x]\).

(iii) Let \(w = c + di\) and \(z = a + bi\) be two elements of \(\mathbb{Z}[i]\) with \(w \neq 0\). Note that \(w\) and \(iw\) are two linearly independent vectors in the plane, so we can write \(z = \alpha w + \beta(iw)\) for some \(\alpha, \beta \in \mathbb{R}\). Find \(m_1, n_1 \in \mathbb{Z}\) such that \(u_1 = \alpha - m_1\) and \(v_1 = \beta - n_1\) have absolute value less than \(1/2\). We have \(z = (m_1 + u_1)w + (n_1 + v_1)iw = (m_1 + n_1)i + (u_1 + v_1)w\). Let \(q = (m_1 + n_1)i\) and \(r = (u_1 + v_1)i\), so \(z = qw + r\). Now, \(z, w, q \in \mathbb{Z}[i]\), so \(r = z - qw \in \mathbb{Z}[i]\). Finally \(r^2 = |u_1 + v_1|^2|w|^2 = (u_1^2 + v_1^2)|w|^2 < |w|^2/2 < |w|^2\). \(\square\)

6.14. Example:
Let \( R = \mathbb{Z}[i] \). We choose two elements \( z, w \in R \). Here \( z = -8 + 5i \) and \( w = 3 + 2i \). The vertices of the square grid shown with solid lines form the ideal \( wR \) generated by \( w \). Given \( z \) and \( w \), we can calculate the quotient and remainder as follows. We calculate \( \frac{z}{w} = \frac{-8+5i}{3+2i} = \frac{-14+31i}{13} \). So \( z = \frac{-14}{13} w + \frac{31}{13} iw = (-1 - \frac{1}{13})w + (2 + \frac{5}{13})iw \). It follows that \( z = qw + r \) where \( q = (-1 + 2i) \) and \( r = (-\frac{1}{13} + \frac{5}{13} i)w \). Note that since \( z, w, q \in R \), we have \( r \in R \). Indeed \( r = (-1 + i) \).

6.15. **Theorem.** Every Euclidean domain is PID.

**Proof.** Generalize the proof that works for \( \mathbb{Z} \) and \( k[x] \). Let \( R \) be an Euclidean domain. Given a nonzero \( I \) in \( R \), pick \( b \in I \setminus \{0\} \) such that \( b \) has minimal Euclidean valuation among all nonzero elements of \( I \). Pick \( a \in I \). Write \( a = bq + r \) for some \( q, r \in R \) such that \( \nu(r) < \nu(b) \) or \( r = 0 \). Since \( a, b \in I \), we have \( r = a - bq \in I \). Since \( b \) has minimal Euclidean valuation among all nonzero elements of \( I \), we must have \( r = 0 \), so \( a = bq \), hence \( a \in bR \). It follows that \( I = bR \) is principal. \( \square \)
7. Gauss Lemma

7.1. Definition. Let $R$ be a domain. Define the field of fractions $F = \text{Frac}(R)$. Note that $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$. If $k$ is a field, then $\text{Frac}(k[x])$ is field of rational functions.

Let $R$ be a domain and $F = \text{Frac}(R)$. We want to compare irreducibility of polynomials in $R[x]$ and irreducibility of the same polynomial considered as an element of $F[x]$. The problem may be more manageable in $F[x]$ since the Euclidean division algorithm works in $F[x]$, so for example, having a linear factor is the same as having a root, which can be tested.

7.2. Lemma. (a) Let $R$ be a commutative ring and $S = R[x]$ be the polynomial ring in one variable $x$ with coefficients in $R$. Let $a \in R$. Then $S/aS \simeq (R/aR)[x]$. In other words, if $f(x) \in R[x]$, then $a$ divides $f(x)$ in $R[x]$ if and only if $a$ divides each coefficient of $f(x)$ in $R$.

(b) If $a$ is a prime in $R$, then $aS$ is a prime in $S$.

Proof. (a) The quotient homomorphism $R \rightarrow R/aR$ induces a homomorphism $\phi : S = R[x] \rightarrow R/aR[x]$ that takes $\sum_j a_j x^j$ to $\sum_j (a_j \mod aR)x^j$. Verify that $\ker(\phi) = aS$. From the first isomorphism theorem, it follows that $S/aS \simeq R/aR[x]$. Let $f \in S$ and $a \in R$. Then $a \mid f$ in $S$ if and only if $f \in aS$, which is equivalent to saying that $\phi(f) = 0$ or in other words, that each coefficient of $f$ is divisible by $a$ in $R$. This proves part (a).

(b) Note that $a$ is a prime in $R$ if and only if $R/aR$ is a domain. Now $R/aR$ is a domain if and only if $R/aR[x]$ is a domain. By part (a), this is equivalent to saying that $S/aS$ is a domain, or that $aS$ is a prime in $S$. \hfill □

7.3. Remark. For the discussion below, let $R$ be a UFD. Fix a set $V$ of prime elements of $R$ such that no two of them are unit multiple of each other, and every prime element in $R$ is a unit multiple of some element of $V$. For any $a \in R$, by unique factorization, we may write $a = u_a \prod_{p \in V} p^{v_p(a)}$ where $u_a$ is a unit, $v_p(a) \in \mathbb{Z}_{\geq 0}$ and $v_p(a) > 0$ for atmost finitely many $p$. Note that the uniqueness of factorization implies that the integers $v_p(a)$ are uniquely determined by $a$.

7.4. Lemma. (a) Let $a, c \in R$. Then $v_p(ac) = v_p(a) + v_p(c)$ for all prime $p \in V$.

(b) Let $a, b \in R$. Then $a \mid b$ if and only if $v_p(a) \leq v_p(b)$ for all $p \in V$.

(c) Let $a_0, \ldots, a_n \in R$. Then $\gcd(a_0, \ldots, a_n)$ exists in $R$ and is unique upto units. For each $p \in V$, let $n_p = \min\{v_p(a_0), \ldots, v_p(a_n)\}$. Then one has $\gcd(a_0, \ldots, a_n) = \prod_{p \in V} p^{n_p}$.

(d) Let $a, a_0, \ldots, a_n \in R$. Then one has $\gcd(aa_0, \ldots, aa_n) = a \gcd(a_0, \ldots, a_n)$.

7.5. Lemma. An element is irreducible in a UFD if and only if it is a prime element.

The proof of the two lemmas above are left as exercises.

7.6. Definition. Let $f(x) \in R[x]$. Define the content of $f(x)$ to be the gcd of all its coefficients. We denote the content of $f(x)$ by $c(f)$. Say that $f(x)$ is primitive, if $c(f) = 1$; otherwise say that $f(x)$ is imprimitive. In other words, $f(x)$ is imprimitive, if there is a non-unit $a \in R$ such that $a$ divides all the coefficients of $f(x)$, or equivalently, $f(x) \in aR[x]$ (by 7.2).

7.7. Lemma. Let $R$ be an UFD. Let $f(x) \in R[x]$ and $a \in R$.

(a) Then $c(af) = ac(f)$ (Caution: Remember that these equations hold only upto units).

(b) One can write $f(x) = c(f)f^*(x)$ where $f^*(x)$ is primitive.
Proof. (a) is immediate from \( \gcd(aa_0, \ldots, aa_n) = a\gcd(a_0, \ldots, a_n) \). By definition of \( c(f) \) we can write \( f(x) = c(f)f_\ast(x) \) for some \( f_\ast(x) \in R[x] \). Now (a) implies \( c(f) = c(f)c(f_\ast) \), so \( c(f_\ast) = 1 \).

7.8. Lemma. Let \( R \) be an UFD. Let \( f(x), g(x) \in R[x] \).

(a) If \( f(x) \) and \( g(x) \) are primitive, then so is \( f(x)g(x) \).

(b) One has \( c(fg) = c(f)c(g) \) (upto units).

Proof. (a) If possible, suppose \( f(x)g(x) \) is not primitive. Then there exists a non-unit \( a \in R \) such that \( f(x)g(x) \in aR[x] \). Let \( p \) be an irreducible (hence prime) factor of \( a \). Then \( f(x)g(x) \in pR[x] \) and \( pR[x] \) is a prime ideal (by 7.2(b)), either \( f(x) \in pR[x] \) or \( g(x) \in pR[x] \). In other words, \( p \) divides each coefficient of \( f(x) \) or \( p \) divides each coefficient of \( g(x) \).

(b) Using 7.8(b), we can write \( fg = c(f)c(g)f_\ast(x)g_\ast(x) \) where \( f_\ast \) and \( g_\ast \) are primitive. So part (a) implies \( c(f_\ast g_\ast) = 1 \). Now 7.8(a) implies \( c(fg) = c(f)c(g)c(f_\ast g_\ast) = c(f)c(g) \).

7.9. Lemma. Let \( R \) be a UFD and let \( F \) be the field of fractions of \( R \). Let \( p(x) \in R[x] \). If \( p(x) \) has a proper factorization \( p(x) = A(x)B(x) \) in \( F[x] \), then \( p(x) \) has a factorization in \( R[x] \) as product of two polynomials of degree \( \deg(A) \) and \( \deg(B) \). In particular, if \( p(x) \) is reducible in \( F[x] \), then \( p(x) \) is reducible in \( R[x] \).

Proof. Suppose \( p(x) = A(x)B(x) \) is a factorization in \( F[x] \), for some \( A(x), B(x) \in F[x] \). There exists \( t_1, t_2 \in R \) such that \( a(x) = t_1A(x) \in R[x] \) and \( b(x) = t_2B(x) \in R[x] \). Let \( t = t_1t_2 \). Then \( tp(x) = a(x)b(x) \) is a factorization in \( R[x] \). Calculating content, we find, \( tc(p) = c(a)c(b) \). Write \( a(x) = c(a)a_\ast(x) \) and \( b(x) = c(b)b_\ast(x) \). Then \( tp(x) = c(a)c(b)a_\ast(x)b_\ast(x) \), so \( p(x) = c(p)a_\ast(x)b_\ast(x) \) is a factorization of \( p(x) \) in \( R[x] \).}

7.10. Corollary. Let \( R \) be a UFD and let \( F \) be the field of fractions of \( R \). Suppose \( f(x) \in R[x] \) and \( c(f) = 1 \). Then \( f \) is irreducible in \( F[x] \) if and only if \( f \) is irreducible in \( R[x] \).

7.11. Theorem. If \( R \) is a UFD, then so is \( R[x] \).

Proof. First one verifies that irreducibles in \( R \) remain irreducible in \( R[x] \).

Let \( F \) be the field of fraction of \( R \). Suppose \( f(x) \in R[x] \). First factorize in \( F[x] \) to write \( f(x) = g_1(x) \cdots g_s(x) \) where \( f_j(x) \) are irreducible polynomials in \( F[x] \). Now clear denominator to find \( t \in R \) such that \( tf(x) = f_1(x) \cdots f_r(x) \) is a factorization in \( R[x] \) and \( f_j \) are multiples of \( g_j \) by elements of \( R \), so \( f_j \)'s are irreducible in \( F[x] \). Now \( tc(f) = c(f_1) \cdots c(f_r) \). So writing \( f_j(x) = c(f_j)f_{j,\ast}(x) \) we get \( f(x) = c(f)f_{1,\ast}(x) \cdots f_{r,\ast}(x) \). Note that \( f_{j,\ast}(x) \) is irreducible in \( F[x] \) (since \( f_j \) is) and \( c(f_j,\ast) = 1 \), so \( f_{j,\ast}(x) \) is irreducible in \( R[x] \). Now factorize \( c(f) \) into irreducibles and we obtain a decomposition of \( f(x) \) into irreducibles.

Suppose \( f(x) = a_1 \cdots a_s f_1(x) \cdots f_r(x) = b_1 \cdots b_t g_1(x) \cdots g_t(x) \) where \( a_j \)'s and \( b_j \)'s are irreducibles in \( R \) and \( f_j \)'s and \( g_j \)'s are irreducibles in \( R[x] \). Then \( c(f_j) = c(g_j) = 1 \) for each \( j \), so \( c(f) = a_1 \cdots a_s \) and by the same token \( c(f) = b_1 \cdots b_t \). Since \( R \) is a UFD, it follows that \( s = t \) and the list of \( a_j \)'s and \( b_j \)'s are the same upto permutation of factors and upto units. So Cancelling these and possibly changing \( f_1 \) by a unit, we get \( f_1(x) \cdots f_r(x) = g_1(x) \cdots g_t(x) \). Since \( f_j \)'s and \( g_j \)'s are irreducible in \( R[x] \), they remain irreducible in \( F[x] \). Since \( F[x] \) is a UFD, it follows that \( tr = l \) and there exists some permutation \( \pi \) such that \( f_j(x) = (m_j/n_j)g_{\pi(j)}(x) \), for some \( m_j, n_j \in R \). So \( n_j c(f_j) = m_j c(g_{\pi(j)}) \). Since \( f_j \) and \( g_j \) are primitive \( m_j/n_j \) is a unit in \( R \) for all \( j \).

The Gauss’ lemma can sometimes be used to show that a polynomial is irreducible over \( \mathbb{Q} \). We give two such results.
7.12. Corollary (Corollary to Gauss’ lemma). Let \( p(x) = \sum_{i=0}^{n} a_i x^i \) be a polynomial in \( \mathbb{Z}[x] \) with \( a_0 \neq 0 \). If \( p \) has a solution in \( \mathbb{Q} \), then it has a solution \( \alpha \in \mathbb{Z} \). Further, \( \alpha \) divides \( a_0 \).

**Sketch of proof.** If \( p \) has a rational solution, then \( p \) factors in \( \mathbb{Q}[x] \) as a product of a polynomial of degree 1 and a polynomial of degree \( \deg(p) - 1 \). By Gauss’ lemma it follows that \( p \) has a factorization in \( \mathbb{Z}[x] \) with a degree one factor. Since \( p \) is monic, one can verify that the linear factor can be chosen to be \( (x - \alpha) \), so \( \alpha \in \mathbb{Z} \) is a root of \( p \) in \( \mathbb{Z} \). Since \( 0 = p(\alpha) = \alpha^n + \cdots + a_1 \alpha + a_0 \), we have \( \alpha \mid a_0 \).

7.13. Remark: Let \( f(x) \in \mathbb{Z}[x] \) and let \( p \) be a prime. Reducing coefficients modulo \( p \), we obtain a polynomial \( f(x) \mod p \in \mathbb{F}_p[x] \). Note that whether \( f(x) \mod p \) has a root in \( \mathbb{F}_p[x] \) or not can be checked by a finite calculation, simply by calculating \( f(x) \mod p \) for \( \{0, 1, \cdots, p - 1\} \). If \( \alpha \) is a root of \( f \) in \( \mathbb{Z} \), then \( \alpha \mod p \) would be a root of \( f(x) \mod p \) in \( \mathbb{F}_p[x] \). So if we can find some prime \( p \) such that \( f(x) \mod p \) does not have a root, then we can conclude that \( f(x) \) does not have a root in \( \mathbb{Z}[x] \). Together with the above corollary, this observation often lets us conclude that some polynomial does not have a degree one factor in \( \mathbb{Q}[x] \).

7.14. Theorem (Eisenstein’s Criteria). Let \( f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \). Suppose there exists a prime \( p \) such that \( p \) divides \( a_0, a_1, \cdots, a_{n-1} \), but \( p \) does not divide \( a_n \) and \( p^2 \) does not divide \( a_0 \). Then \( f(x) \) is irreducible over \( \mathbb{Q}[x] \).

**Proof.** By Gauss’ lemma it suffices to show that \( f(x) \) cannot be factored into two polynomials of lower degree in \( \mathbb{Z}[x] \). Suppose \( f(x) = (b_s x^r + \cdots + b_0)(c_s x^s + \cdots + c_0) \) be a factorization in \( \mathbb{Z}[x] \) with \( r, s \geq 1 \) and \( b_s, c_s \neq 0 \). Note that \( a_0 = b_0 c_0 \) is divisible by \( p \) but not divisible by \( p^2 \). Without loss, we may assume that \( p \) divides \( c_0 \) and does not divide \( b_0 \). Note that \( p \) does not divide \( c_s \) since \( p \) does not divide \( a_n = b_s c_s \). Since \( p \) divides \( c_0 \) and does not divide \( c_s \), there exists an integer \( m \leq s \) such that \( p \) divides \( c_0, c_1, \cdots, c_{m-1} \) but \( p \) does not divide \( c_m \). Now note that \( a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0 \) is not divisible by \( p \) since each term except the first term in the sum is divisible by \( p \) except \( b_0 c_m \). This is a contradiction since \( m \leq s < n \) and we are given that \( a_0, \cdots, a_{n-1} \) are all divisible by \( p \).

Here is a slightly non-trivial application of Eisenstein’s criteria.

7.15. Corollary. Let \( p \) be a prime. The polynomial \( f(x) = 1 + x + \cdots + x^{p-1} \) is irreducible in \( \mathbb{Q}[x] \).

**Proof.** One has \((x - 1)f(x) = (x^p - 1)/(x - 1)\). Let \( y = x - 1 \). Then using Binomial theorem, we get

\[
f(y + 1) = \frac{(y + 1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{1}.
\]

Note that all the binomial coefficients are divisible by \( p \) and the constant term is not divisible by \( p^2 \). By Eisenstein’s Criteria, we conclude that \( f(y + 1) \) is irreducible over \( \mathbb{Q}[x] \). Hence so is \( f(x) \).
8. **Vector Spaces**

8.1. **Definition.** For this whole section $F$ will denote a field. A vector space $V$ over $F$ is an abelian group $V = (V, +, 0)$ together with a map $F \times V \to V$ written $(\alpha, v) \mapsto \alpha v$, satisfying $1v = v$, $\alpha(\beta v) = (\alpha\beta)v$, $(\alpha + \beta)v = \alpha v + \beta v$, $\alpha(v + w) = \alpha v + \beta w$. In this context the elements of $F$ are called scalars and the map $(\alpha, v) \mapsto \alpha v$ is called the scalar multiplication and the elements of $V$ are called vectors. A subset $U$ of $V$ is called a *subspace* if $U$ is a vector space in its own right with the operations induced from $V$. Verify that a subset $U$ of $V$ is a subspace if and only if $0 \in U$ and $U$ is closed under addition and scalar multiplication, that is, $u, v \in U$ implies $u + v \in U$ and $u \in U$ and $\alpha \in F$ implies $\alpha u \in U$.

In the following definitions, let $V$ be a vector space over $F$ and let $v_1, \ldots, v_m \in V$. A *linear combination* of $v_1, \ldots, v_m$ is a vector in $V$ of the form $(\alpha_1 v_1 + \cdots + \alpha_m v_m)$ for some scalars $\alpha_1, \ldots, \alpha_m$. We say that $(\alpha_1 v_1 + \cdots + \alpha_m v_m)$ is a non-trivial linear combination of $v_1, \ldots, v_m$ if at least some $\alpha_j$ is non-zero. Verify that the set of all linear combination of the $v_1, \ldots, v_m$ forms the smallest subspace of $V$ containing $\{v_1, \ldots, v_m\}$; it is called the *span* of $v_1, \ldots, v_m$. So an vector $v$ belongs to the span of $v_1, \ldots, v_m$ if and only if $v$ can be written as a linear combination of $v_1, \ldots, v_m$. Say that $V$ is a *finite dimensional* vector space (over $F$) if $V$ has a finite spanning set.

Say that $v_1, \ldots, v_m$ are *linearly dependent* if a non-trivial linear combination of $v_1, \ldots, v_m$ is equal to zero. Verify that this is equivalent to saying that at least some $v_j$ can be written as a linear combination of the rest of vectors $\{v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_m\}$. Say that $v_1, \ldots, v_m$ are *linearly independent* if $v_1, \ldots, v_m$ are not linearly dependent. In other words, $v_1, \ldots, v_m$ are linearly independent if $\sum_j \alpha_j v_j = 0$ for some scalars $\alpha_1, \ldots, \alpha_m$ implies $\alpha_1 = \cdots = \alpha_m = 0$. A subset $B$ of $V$ is called a *basis* of $V$ if $B$ is linearly independent and $B$ spans $V$. Verify that $B = \{b_1, \ldots, b_n\}$ is a basis of $V$ if and only if every $v \in V$ can be expressed as a linear combination $v = \sum_{i=1}^n \alpha_i b_i$ for some scalars $\alpha_1, \ldots, b_n$ that are uniquely determined by $v$. The scalar $\alpha_i$ is called the coefficient of $b_i$ in the above linear combination.

8.2. **Example.** Let $F^n$ be the rank $n$ free module over $F$ consisting of all row vectors of length $n$ with entries from $F$. Let $e_j$ be the vector whose $j$-th entry is $1$ and all other entries are zero. Then verify that $\{e_1, \ldots, e_n\}$ is a basis of $F^n$. This is called the *standard basis* of $F^n$.

8.3. **Lemma.** Let $v_0, v_1, \ldots, v_n \in V$. Then the following are equivalent:

(a) $v_0$ is a linear combination of $v_1, \ldots, v_n$.

(b) $\text{span}\{v_1, \ldots, v_n\} = \text{span}\{v_0, \ldots, v_n\}$.

*Proof.* Clearly (b) implies (a). Now assume (a). By (a), we can write $v_0 = \beta_1 v_1 + \cdots + \beta_n v_n$ for some scalar $\beta_1, \ldots, \beta_n$. Suppose $v \in \text{span}\{v_0, \ldots, v_n\}$. Then $v$ can be written as $v = \alpha_0 v_0 + \alpha_1 v_1 + \cdots + \alpha_n v_n$ for some scalars $\alpha_j$. Then $v = (\alpha_1 + \alpha_0 \beta_1) v_1 + \cdots + (\alpha_n + \alpha_0 \beta_n) v_n$, so $v \in \text{span}\{v_1, \ldots, v_n\}$. It follows that $\text{span}\{v_0, v_1, \ldots, v_n\} \subseteq \text{span}\{v_1, \ldots, v_n\}$; the other inclusion is obvious. So (a) implies (b). $\square$

8.4. **Lemma.** Let $V$ be a vector space and let $B = \{b_1, \ldots, b_n\} \subseteq V$. Then the following are equivalent

(a) $B$ is a maximal linearly independent set.

(b) $B$ is a minimal spanning set.

(c) $B$ is a basis of $V$.
Proof. Assume (a). If $B$ does not span $V$, then choose $v \in V \setminus \text{span}(B)$. We claim that $B \cup \{v\}$ is also linearly independent. Suppose $\alpha_0 v + \sum_{i=1}^n \alpha_i b_i = 0$. Observe that $\alpha_0 \neq 0$ would imply that $v$ is a linear combination of $b_1, \ldots, b_n$, contradicting the assumption $v \notin \text{span}(B)$, so $\alpha_0$ must be 0. But then we get $\sum_{i=1}^n \alpha_i b_i = 0$ and since $b_1, \ldots, b_n$ are linearly independent, it follows that $\alpha_1 = \cdots = \alpha_n = 0$. So $B \cup \{v\}$ is also linearly independent, which contradicts the assumption in (a). Thus (a) implies (b).

Assume (b). If $B$ is not linearly independent, then we have a relation of the form $\alpha_1 b_1 + \cdots + \alpha_n b_n = 0$, with some $\alpha_i \neq 0$. Then $b_i$ can be written as a linear combination of $\{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n\}$ and it follows from the previous lemma that $\{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n\}$ also spans $V$ contradicting the assumption in (b) that $B$ is a minimal spanning set. So $B$ must be linearly independent as well. Thus (b) implies (c).

Now assume (c). Then $B$ is linearly independent. Take $v \in V \setminus B$. Since $B$ spans $V$, we can write $v = \sum_i \alpha_i b_i$ for some scalars $\alpha_j$, so $\{v, b_1, \ldots, b_n\}$ is not linearly independent. So $B$ is maximal linearly independent set. Thus (c) implies (a). \hfill $\square$

8.5. Corollary. If $V$ is a finite dimensional vector space, then $V$ has a finite basis.

Proof. Choose a spanning subset $X$ of $S$ with least number of elements; then $X$ is a basis. \hfill $\square$

Infact Zorn’s lemma can be used to show that any vector space has a basis.

8.6. Lemma. Suppose $B$ is a finite basis of $V$. Suppose $b \in B$ such that when $v$ is written as a linear combination of the elements of $B$, the coefficient of $b$ is non-zero. Then $(B \setminus \{b\}) \cup \{v\}$ is also a basis of $V$.

Proof. Name the elements of $B$ so that $B = \{b_1, \ldots, b_n\}$ such that $b = b_1$. We know $v$ can be written as $v = \sum_i \alpha_i b_i$ for some scalars $\alpha_j$, with $\alpha_1 \neq 0$. Then $b_1 = \alpha_1^{-1}(v - \alpha_2 b_2 - \cdots - \alpha_n b_n)$, so $b_1 \in \text{span}\{v, b_2, \ldots, b_n\}$, so $V = \text{span}\{b_1, \ldots, b_n\} \subseteq \text{span}\{v, b_2, \ldots, b_n\}$. So $\{v, b_2, \ldots, b_n\}$ spans $V$. Suppose $\beta_1 v + \beta_2 b_2 + \cdots + \beta_n b_n = 0$ for some scalars $\beta_j$. Then substituting the expression for $v$ in terms of $b_1, \ldots, b_n$, we get $\beta_1 \alpha_1 b_1 + (\beta_2 + \beta_1 \alpha_2)b_2 + \cdots +(\beta_n + \beta_1 \alpha_n)b_n = 0$. Since $B$ is linearly independent, each coefficient in the above expression must be zero, so $\beta_1 \alpha_1 = 0$. Since $\alpha_1 \neq 0$, we get $\beta_1 = 0$. Now it follows that $\beta_2 = \cdots = \beta_n = 0$ as well. So $\{v, b_2, \ldots, b_n\}$ are linearly independent. \hfill $\square$

8.7. Lemma. Let $\{v_1, \ldots, v_s, \ldots, v_k\}$ be a linearly independent set and Suppose $B = \{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ be a basis of $V$. Then there exists $1 \leq j \leq r$ such that $(B \setminus \{u_j\}) \cup \{v_{s+1}\}$ is also a basis of $V$.

Proof. Write $v_{s+1} = (\lambda_1 u_1 + \cdots + \lambda_r u_r) + (\mu_1 v_1 + \cdots + \mu_s v_s)$. Since the $v_i$’s are linearly independent, $\lambda_j \neq 0$ for some $j$. Pick just a $j$. Then apply 8.6. \hfill $\square$

8.8. Lemma. Let $\{v_1, \ldots, v_k\}$ be a linearly independent set and Suppose $B = \{u_1, \ldots, u_m\}$ be a basis of $V$. Then there is a $k$ element subset $B_0$ of $B$ such that $(B \setminus B_0) \cup \{v_1, \ldots, v_k\}$ is a basis of $V$.

Proof. Apply 8.7 $k$ times to replace $k$ of the $u_j$’s with $v_1, \ldots, v_k$ successively in the basis. \hfill $\square$

8.9. Lemma. Any linearly independent set in a finite dimensional vector space $V$ can be extended to a basis of $V$.

Proof. Follows from the 8.8 since every finite dimensional vector space has a finite basis. \hfill $\square$
8.10. **Theorem.** Suppose $V$ is finite dimensional. Then there is a number $n$ such that any basis of $V$ has $n$ elements. This number $n$ is called the dimension of $V$. We write $\dim(V) = n$.

**Proof.** Suppose $B = (b_1, \ldots, b_n)$ and $C = (v_1, \ldots, v_k)$ be two bases of $V$. Without loss, suppose $k \leq n$. Then 8.8 implies that $B' = (B \setminus B_0) \cup C$ is a basis of $V$ where $|B_0| = k$. But $C$ already a basis, so a maximal linearly independent set, so if $B'$ properly contains $C$, it cannot be a basis. It follows that $B \setminus B_0 = \emptyset$, so $k = n$. \qed
10. **Field extensions**

**Notation:** The letters $F, K, L, M$ would usually denote fields.

10.1. **Definition.** Let $F$ be a field. The *characteristic* of a field, denoted $\text{ch}(F)$ is the smallest natural number $n$ such that $n \cdot 1_F = 0$. If no such $n$ exists, then one says that $F$ has characteristic zero, otherwise one says that $F$ has finite characteristic. If $F$ is finite characteristic, then it is easy to see that $\text{ch}(F)$ is a prime number.

Clearly the intersection of a collection of subfields of $F$ is again a subfield. If $F$ is a field and $S$ is some subset of $F$, then the *subfield of $F$ generated by $S$* is defined to be the intersection of all subfields of $F$ that contain $S$. So the subfield of $F$ generated by $S$ is the smallest subfield of $F$ that contains $S$.

The *prime subfield* of $F$ is defined to be the subfield generated by $1_F$. If $F$ has characteristic zero, then the prime subfield is isomorphic to $\mathbb{Q}$. If $F$ has characteristic $p$, then the prime subfield is isomorphic to $\mathbb{F}_p$.

10.2. **Theorem.** Let $p(x)$ be a non-constant polynomial in $F[x]$. Then one can construct a field $E$ such that $F \subseteq E$ and such that $p(x)$ has a root in $E$.

10.3. **Field extensions:** If $K$ is a field containing a field $F$, then we say that $K$ is an *extension field* of $F$. We use the shorthand $K/F$ to denote a field extension. Two extensions $K/F$ and $K'/F$ are called *isomorphic* if there is a field isomorphism $\phi : K \rightarrow K'$ such that the restriction of $\phi$ to $F$ is the identity.

If $F \subseteq K \subseteq M$ is a “tower” of extensions, we say that $K/F$ is a *subextension* of $M/F$.

If $K/F$ is an field extension, then $K$ is a $F$-vector space. The dimension of this vector space is called the *degree* of the extension and denoted by $[K : F] = \dim_F(K)$. We say that $K/F$ is a *finite extension* if $[K : F]$ is finite.

An element $a \in K$ called *algebraic* over $F$ if there exists $p(x) \in F[x]$ such that $p(a) = 0$. Call $K/F$ an *algebraic* extension if each element of $K$ is algebraic over $F$.

10.4. **Theorem.** Suppose $F \subseteq K \subseteq M$ is a tower of extensions. Then $M/F$ is finite if and only if $M/K$ and $K/F$ are both finite.

Suppose $a_1, \ldots, a_m$ be a basis of $K/F$ and let $b_1, \ldots, b_n$ be a basis of $M/F$. Then the \{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\} forms a basis of $M/K$. So $[M : F] = [M : K][K : F]$.

**Proof.** Exercise.

10.5. **Theorem.** Finite extensions are algebraic.

**Proof.** Let $K/F$ be a finite extension and $a \in K$. The elements $1, a, a^2, \ldots$ cannot be all linearly independent over $F$, so some nontrivial linear combination of these must be zero. In other words, $a$ must satisfy of some polynomial with coefficients in $F$. 

10.6. **Minimal polynomials:** Suppose $K/F$ is an algebraic extension and $a \in K$. Let $F[a]$ and $F(a)$ be respectively the subring and subfield of $K$ generated by $F$ and $a$. Let $\phi_a : F[x] \rightarrow F[a]$ be the surjective homomorphism obtained by sending $x$ to $a$. Then $\ker(\phi_a) = \{f \in F[x] : f(a) = 0\}$ is an ideal in $F[a]$. Since $a$ is algebraic over $F$, the ideal $\ker(\phi_a)$ is not zero. So there exists a unique monic polynomial $p_a(x)$ such that $\ker(\phi_a) = \langle p_a(x) \rangle$. Verify that $p_a(x)$ is the unique monic polynomial in $F[x]$ of minimal degree such that $p_a(a) = 0$. We call $p_a(x)$ the *minimal polynomial* of $a$ (over $F$). Thus we have

$$0 \rightarrow (p_a(x)) \rightarrow F[x] \xrightarrow{\phi_a} F[a] \rightarrow 0,$$

where $\phi_a(x) = a$. 

Recall that in a PID every prime ideal is maximal. Since $F[a] \simeq F[x]/(p_a)$ is an integral domain, $(p_a)$ is a prime ideal, hence maximal. So $F[a] \simeq F[x]/(p_a)$ is actually a field. So
$$F[x]/(p_a) \simeq F[a] = F(a).$$

If the polynomial $p_a$ has degree $d$ then one verifies that $1, a, a^2, \ldots, a^{d-1}$ forms a basis of $F(a)$ as a $K$ vector space. Hence $[F(a) : F] = d$. Conversely we have the following:

10.7. **Theorem.** Let $p$ be an irreducible monic polynomial of degree $d$ in $F[x]$. Then there exists a extension $K/F$ of degree $d$ and $a \in K$ such that $p$ is the minimal polynomial of $a$ and $K = F[a] \simeq F[x]/(p(x))$.

Suppose $K$ and $K'$ are two extensions of $F$ and $a \in K$, $a' \in K'$ such that $p(x)$ is the minimal polynomial of $a$ and $a'$ over $F$. Then the extensions $K/F$ and $K'/F$ are isomorphic via an isomorphism that sends $a$ to $a'$.

**Proof.** Since $p(x)$ is irreducible, it is a prime. In a PID every prime ideal is maximal, so $K = F[x]/(p)$ is a field. Let $\phi : F[x] \rightarrow F[x]/(p)$ be the surjection. If $f(x) \in F[x]$ then $\phi(f(x)) = f(x) \mod (p) = f(x \mod (p)) = f(\phi(x))$. The composition
$$F \rightarrow F[x] \xrightarrow{\phi} K = F[x]/(p)$$
is injective (since $F$ is a field and the kernel of the composite is not the whole of $F$, hence must be zero). Identify $F$ with the image of of this injection. In other words, we make the identification $\phi(\alpha) = \alpha$ where $\alpha \in F$ is a scalar. Then $K/F$ is a field extension and we can consider $p(x)$ to be a polynomial in $F[x]$. For $f(x) = \sum_i \alpha_i x^i \in F[x]$, note that
$$\phi(f(x)) = \phi(\sum_i \alpha_i x^i) = \sum_i \phi(\alpha_i) \phi(x)^i = \sum_i \alpha_i \phi(x)^i = f(\phi(x)).$$
where the second equality follows since $\phi$ is a ring homomorphism and the third one uses the identification $\phi(F) = F$.

Let $a = \phi(x)$. Then $K = F[a]$ and $p(a) = p(\phi(x)) = \phi(p(x)) = 0$ holds in $K$. Since $p(x)$ is irreducible, it must be the minimal polynomial of $a$. Finally, $1, a, a^2, \ldots, a^{d-1}$ is a basis of $K$ as a $F$-vector space. \hfill $\square$

10.8. **Generators for a field extension:** Let $F[x_1, \ldots, x_n]$ denote the ring of polynomials in $n$ variables $x_1, \ldots, x_n$, with coefficients in the field $F$. The fraction field of $F[x_1, \ldots, x_n]$ is the field of all rational functions, denoted by $F(x_1, \ldots, x_n)$.

Let $K/F$ be a field extension and $a_1, \ldots, a_n \in K$. Then one verifies that the smallest subfield of $K$ generated by $F$ and $a_1, \ldots, a_n$ consists of all rational expressions of the form $f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n)$ where $f, g \in F[x_1, \ldots, x_n]$ and $g(a_1, \ldots, a_n) \neq 0$. This field is denoted by $F(a_1, \ldots, a_n)$. Say that the extension $K/F$ is generated by $a_1, \ldots, a_n \in K$ if $K = F(a_1, \ldots, a_n)$. Say that an extension $K/F$ is finitely generated if $K = F(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n$. Observe that
$$F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n).$$
Say that $K/F$ is a simple extension if $K = F(a)$ for some $a \in K$.

10.9. **Theorem.** Let $K/F$ be an extension. Then the following are equivalent:

(a) $K/F$ is a finite extension. par (b) There exists finitely many elements $a_1, \ldots, a_n \in K$ such that each $a_j$ is algebraic over $F$ and $K = F(a_1, \ldots, a_n)$.
(c) There exists \( a_1, \ldots, a_n \in K \) such that \( K = F(a_1, \ldots, a_n) \) and \( a_i \) is algebraic over \( F(a_1, \ldots, a_{i-1}) \) for each \( i \).

**Proof.** Suppose \( K/F \) is finite. Let \( a_1, \ldots, a_n \) be a basis of \( K \) as a \( F \)-vector space. Since finite extensions are algebraic, each \( a_j \) is algebraic over \( F \) and \( a_1, \ldots, a_n \) generate \( K \) as a \( F \)-vector space, hence also as a field, that is, \( F(a_1, \ldots, a_n) = K \). Thus (a) implies (b).

Suppose \( a_1, \ldots, a_n \in K \) such that each \( a_j \) is algebraic over \( F \) and \( K = F(a_1, \ldots, a_n) \). Let \( m_j \) be the degree of the minimal polynomial of \( a_j \) over \( F \). A fortiori, \( a_j \) satisfies a polynomial of degree \( m_j \) which has coefficients in \( F(a_1, \ldots, a_{j-1}) \). So \( [F(a_1, \ldots, a_{j-1})(a_j), F(a_1, \ldots, a_{j-1})] \leq m_j \). Thus (b) implies (c).

Now assume (c). Then every step in the tower
\[
F \subseteq F(a_1) \subseteq F(a_1, a_2) \subseteq \cdots \subseteq F(a_1, \ldots, a_n)
\]
is finite and 10.4 implies that \( F(a_1, \ldots, a_n)/F \) is finite too. \( \square \)

10.10. **Corollary.** (a) Let \( F \subseteq K \subseteq M \) be fields. If \( K/F \) and \( M/K \) are algebraic then so is \( M/F \).

(b) Let \( K/F \) be an extension and \( a, b \in K \) are algebraic over \( F \). Then \( (a + b) \) and \( ab \) are also algebraic over \( F \). So the set of elements in \( K \) that are algebraic over \( F \) form a subextension of \( K/F \).

**Proof.** (a) Let \( a \in M \). Then there is a polynomial \( f(x) = \sum_{i=0}^{n} a_i x^i \in K[x] \) such that \( f(a) = 0 \). So \( a \) is algebraic over \( L = F(a_0, \ldots, a_n) \), so \( L(a)/L \) is finite. Since each \( a_j \in K \) is algebraic over \( F \), 10.9 implies that the extension \( L/F \) is finite. So \( L(a)/F \) is also finite and hence \( a \) is algebraic over \( F \).

(b) Since \( a \) and \( b \) are algebraic over \( F \), the extension \( F(a, b)/F \) is finite. Since \( (a + b) \) belong to \( F(a, b) \), the extensions \( F(a + b)/F \) is also finite. Hence \( a + b \) is also algebraic over \( F \). Similar argument for \( ab \). \( \square \)

10.11. **Definition.** Let \( K, K_1, K_2, F \) be fields such that \( F \subseteq K_j \subseteq K \) for \( j = 1, 2 \). Then we define \( K_1K_2 \) to be the subfield generated by \( K_1 \) and \( K_2 \), that is, the smallest subfield of \( K \) that contains both \( K_1 \) and \( K_2 \). We say that \( K_1K_2 \) is the *compositum* of \( K_1 \) and \( K_2 \).

**Exercise:** If \( [K_1 : F] \) and \( [K_2 : F] \) are finite, then \( [K_1K_2 : F] \leq [K_1 : F][K_2 : F] \).

10.12. **Definition.** An injective homomorphism of fields is called an *embedding* of fields. Let \( \sigma : F \to L \) be a homomorphism of fields. Since \( F \) does not have any nonzero ideal, \( \ker(\sigma) \) is either 0 or is equal to \( F \). So either \( \sigma = 0 \) or \( \sigma \) is an embedding. Let \( K/F \) be an extension and \( \sigma : F \to L \) be an embedding. We say that \( \sigma \) *extends to \( K \)* if there exists a field homomorphism \( \sigma' : K \to L \) such that \( \sigma'|_F = \sigma \).

Let \( R, S \) be rings. Any ring homomorphism \( \sigma : R \to S \) induces a ring homomorphism \( R[x] \to S[x] \) by defining \( \sigma(\sum_i a_i x^i) = \sum_i \sigma(a_i) x^i \). This homomorphism \( R[x] \to S[x] \) will again be denoted by \( \sigma \).
11. splitting field, Algebraic closure

11.1. Definition. Let \( f(x) \in F[x] \). Say that \( f(x) \) splits in \( F[x] \) if it can be decomposed into linear factors in \( F[x] \). An extension \( K/F \) is called a splitting field of some non-constant polynomial \( f(x) \) if \( f(x) \) splits in \( K[x] \) but \( f(x) \) does not split in \( M[x] \) for any any \( K \supseteq M \supseteq F \). If an extension \( K \) of \( F \) is the splitting field of a collection of polynomials in \( F[x] \), then we say that \( K/F \) is a normal extension.

11.2. Lemma. Let \( p(x) \) be a non-constant polynomial in \( F[x] \). Then there is a finite extension \( M \) of \( F \) such that \( p(x) \) splits in \( M \).

Proof. Induct on \( \deg(p) \); the case \( \deg(p) = 1 \) is trivial. If \( p \) is already split over \( F \), then \( F \) is already a splitting field. Otherwise, choose an irreducible factor \( p_1(x) \) of \( p(x) \) such that \( \deg(p_1(x)) \geq 1 \). By, there is a finite extension \( M_1/F \) such that \( p_1 \) has a root \( \alpha \) in \( M_1 \). So we can write \( p(x) = (x - \alpha)q(x) \) in \( M_1[x] \). Since \( \deg(q) < \deg(p) \), by induction, there is a finite extension \( M/M_1 \) such that \( q \) splits in \( M \). Then \( M/F \) is also finite and \( p \) splits in \( M \) . □

11.3. Lemma. Let \( \sigma : F \to L \) be an embedding of a field \( F \) into a field \( L \). Let \( p(x) \in F[x] \) be an irreducible polynomial and let \( K = F[x]/(p(x)) \) be the extension of \( F \) obtained by adjoining a root of \( p \). The embedding \( \sigma \) extends to \( K \) if and only if \( \sigma(p)(x) \) has a root in \( L \).

Proof. Let \( a \) be the image of \( x \) in \( K \). So \( K = F[a] = F(a) \simeq F[x]/(p(x)) \). If \( \tilde{\sigma} \) is an extension of \( \sigma \) to \( K \) then \( \tilde{\sigma}(a) \) is a root of \( \sigma(p) \) in \( F \). Conversely, suppose \( \alpha \) is a root of \( \sigma(p) \) in \( L \). Then define a map \( \sigma_1 : F[x] \to L \) such that \( \sigma_1[F] = \sigma \) and \( \sigma_1(x) = \alpha \). Then \( \sigma_1(p(x)) = \sigma(p)(\alpha) = 0 \), so \( \ker(\sigma_1) \) contains \( (p(x)) \) which is a maximal ideal in \( F[x] \). Since \( \sigma_1 \neq 0 \), it follows that \( \ker(\sigma_1) = (p(x)) \). So \( \sigma_1 \) induces an embedding \( \tilde{\sigma} : F[x]/(p(x)) \to L \) which extends \( \sigma \). □

11.4. Theorem. (a) Let \( p(x) \) be a non-constant polynomial in \( F[x] \). Then there is a finite splitting field \( K \) for \( p(x) \).

(b) Any such \( K \) is a finite extension of \( F \).

(c) The splitting field for \( p(x) \) is unique in the sense that if \( K \) and \( K' \) are two splitting fields for \( p(x) \), then \( K/F \) and \( K'/F \) are isomorphic extensions.

Proof. (a) By 11.2 that there is a finite extension \( M \) of \( F \) such that \( p(x) \) splits in \( M \). Let \( K \) be the intersection of all subextensions of \( M/F \) in which \( p(x) \) is split. Verify that \( K \) is a splitting field for \( p(x) \).

(b) let \( K \) be a splitting field of \( p(x) \). Suppose \( p(x) \) factors in \( K \) as \( p(x) = c \prod_{i=1}^{n} (x - a_i) \). Since \( p(x) \) already splits in \( F(a_1, \ldots, a_n) \subseteq K \), we must have \( K = F(a_1, \ldots, a_n) \). Since each \( a_i \) is algebraic over \( F \), the extension \( F(a_1, \ldots, a_n)/F \) is finite.

(c) Let \( i' : F \to K' \) be the inclusion map. Consider the collection of all fields \( M \) such that \( F \subseteq M \subseteq K \) and there exists an embedding \( \sigma : M \to K' \) that extends \( i' \). Among these, choose an \( M \) such that \( [M : F] \) is maximal. Let \( \sigma : M \to K' \) be an extension of \( i' \). We claim that \( M = K \).

Proof of claim: If \( M \neq K \), then there exists a root \( a \in K \) of \( p(x) \) such that \( a \notin M \). Let \( q(x) \) be the minimal polynomial of \( a \) in \( M[x] \). Then \( q(x) \) is a factor of \( p(x) \) in \( M[x] \), hence \( \sigma(q(x)) | \sigma(p(x)) = i'(p(x)) = p(x) \) in \( K'[x] \). But \( p(x) \) splits in \( K'[x] \). So \( \sigma(q(x)) \) has a root in \( K' \). By lemma 11.3, the embedding \( \sigma \) can be extended to \( M(a) \simeq M[x]/(q(x)) \). This contradicts the maximality of \( M \) and proves the claim.

32
Identify \( F \) inside \( K \) and \( K' \). Then, by the claim, we have an embedding \( \sigma : K \to K' \) such that \( \sigma|_F = id_F \). Since \( \sigma(K)/F \) and \( K/F \) are isomorphic extensions, the polynomial \( p(x) \) splits already in \( \sigma(K) \subseteq K' \). Since \( K' \) is a minimal extension in which \( p \) splits, we must have \( \sigma(K) = K' \).

11.5. Definition. Say that a field \( K \) is algebraically closed, if every polynomial in \( K[x] \) splits in \( K \). For example, the fundamental theorem of algebra states that \( \mathbb{C} \) is algebraically closed. An extension \( K \) of \( F \) is called an algebraic closure of \( F \), if \( K/F \) is algebraic extension and \( K \) is algebraically closed.

11.6. Theorem. Let \( L/F \) be an extension with \( L \) algebraically closed. Let \( K/F \) be an algebraic extension. Then there exists an embedding \( \sigma : K \to L \) fixing \( F \).

Proof. Let \( i : F \to L \) be the inclusion map. Consider the collection
\[
\mathcal{F} = \{(M, \sigma) : F \subseteq M \subseteq K, \sigma : M \to K', \sigma|_F = i\}.
\]

Define a partial order on \( \mathcal{F} \) by defining \((M, \sigma) \leq (M', \sigma')\) if and only if \( M \subseteq M' \) and \( \sigma'|_M = \sigma \). One verifies that every chain in \( \mathcal{F} \) has an upper bound. So by Zorn’s lemma, there exists a maximal element \((M, \sigma)\) in \( \mathcal{F} \). We claim that \( M = K \). The proof of this claim is similar to the proof of the claim in 11.4(c).

11.7. Theorem. Every field has an algebraic closure. The algebraic closure is unique in the sense that if \( K \) and \( K' \) are two algebraic closures of \( F \), then the extensions \( K/F \) and \( K'/F \) are isomorphic.

The proof is omitted.

11.8. Definition. Let \( K/F \) be an extension and \( \{f_i : i \in I\} \) be a collection of polynomials in \( F[x] \). We say that \( K \) is a splitting field for the family \( \{f_i : i \in I\} \), if each \( f_i \) splits in \( K \) and \( K \) is a minimal extension with this property. In other words, \( K \) contains all the roots of all the polynomials in \( \{f_i : i \in I\} \) and \( K \) is generated by these roots over \( F \). This field \( K \) contains \( \bar{K} \) for each \( f_i \) and \( K \) is the compositum of the \( \bar{K}_i \)’s.

Let \( M \) be any splitting field of \( \{f_i : i \in I\} \). Fix an algebraic closure \( 
 M \) of \( M \). Then \( M \) is the subfield of \( \bar{M} \) generated over \( F \) by all the roots of all the polynomials in \( \{f_i : i \in I\} \). One verifies that \( M \) is the unique subfield of \( \bar{M} \) that is a splitting field for \( \{f_i : i \in I\} \).

Let \( K \) be any splitting field for \( \{f_i : i \in I\} \). Then 11.6 implies that we have an embedding \( \sigma : K \to \bar{F} \) fixing \( F \). The image \( \sigma(K) \) is a subfield of \( \bar{F} \) and a splitting field of \( \{f_i : i \in I\} \).

So \( \sigma(K) = M \). So splitting field of \( \{f_i : i \in I\} \) is an unique extension of \( F \) upto isomorphism.

11.9. Lemma. Let \( K/F \) be an algebraic extension. Let \( \sigma : K \to K \) be an embedding fixing \( F \). Then \( \sigma \) is an automorphism of \( K \).

Proof. Let \( a \in K \) and let \( p(x) \in F[x] \) be the minimal polynomial of \( a \). Consider the subfield \( M \) of \( K \) generated by all the roots of \( p \) that lie in \( K \). Then restriction \( \sigma|_M \) takes \( M \) to itself since a root of \( p \) maps to a root of \( p \) under \( \sigma \). But \( [M : F] \) is a finite extension and any injective map of finite dimensional vector spaces is an isomorphism. So \( \sigma|_M \) is an isomorphism. So \( a \) is in the image of \( \sigma \), hence \( \sigma \) is an onto.

11.10. Theorem. Let \( K \) be an algebraic extension of \( F \). Fix an algebraic closure \( \bar{F} \) of \( F \) containing \( K \). Then the following conditions are equivalent:

(a) Every embedding of \( K \) into \( \bar{F} \) fixing \( F \) induces an automorphism of \( K \).
(b) $K$ is a splitting field of a family of polynomials $\{f_i : i \in I\}$ in $F[x]$.

(c) Every irreducible polynomial in $F[x]$ which has a root in $K$ splits in $K$.

Proof. Assume (a). Let $a \in K$ and $p_a \in F[x]$ is the minimal polynomial of $a$ over $F$. Let $b$ be a root of $p_a$ in $\bar{F}$. Then there is an isomorphism $F(a) \to F(b)$ mapping $a$ to $b$ whose restriction to $F$ is the identity. Extend this to an embedding $\sigma : K \to \bar{F}$. By our assumption this embedding is an automorphism of $K$, so $\sigma(a) = b$ belongs to $K$. Thus every root of $p_a$ belongs to $K$. So $K$ is the splitting field of the family $\{p_a(x) : a \in K \setminus F\}$. Thus (a) implies (b) and (c).

Assume (b). Then verify that any embedding $\sigma : K \to \bar{F}$ maps $K$ to itself. Then 11.9 shows that $\sigma$ is an automorphism. So (b) implies (a).

Assume (c). Let $a \in K$ and $p(x)$ is the irreducible polynomial of $a$ over $F$. Let $\sigma : K \to \bar{F}$ be an embedding fixing $F$. Then $\sigma(a)$ is another root of $p(x)$, which also belongs to $K$, so $\sigma(K) \subseteq K$. Now, 11.9 implies $\sigma$ is an automorphism of $K$. \qed
12. Finite fields

12.1. Lemma. Let \( f(x) \in F[x] \). The polynomial \( f(x) \) has a repeated root in some extension \( K/F \), if and only if \( f(x) \) and \( f'(x) \) are not relatively prime in \( F[x] \).

Proof. Let \( h(x) \) be a nontrivial common factor of \( f(x) \) and \( f'(x) \). Let \( K \) be an extension of \( F \) where \( h(x) \) has a root \( a \). So \( f(a) = f'(a) = 0 \) in \( K \). Let \( g(x) = f(x)/(x-a) \in K[x] \). By Euclidean algorithm, we can write \( g(x) = q(x)(x-a) + r \) for some \( r \in K \). So \( f(x) = q(x)(x-a)^2 + r(x-a) \) and \( f'(x) = q'(x)(x-a)^2 + 2q(x)(x-a) + r \). Evaluating at \( a \), we get \( 0 = f'(a) = r \), so \( f(x) = (x-a)^2q(x) \), that is, \( f(x) \) has a repeated root in \( K \).

Suppose \( f \) and \( f' \) has no common factor, so \( \gcd(f, f') = 1 \). So there exists \( g, h \in F[x] \) such that \( gf + hf' = 1 \). If \( a \) is a repeated root of \( f(x) \) in some extension \( K \), then \( f(x) = (x-a)^2g(x) \) in \( K[x] \), so \( (x-a) \) divides both \( f \) and \( f' \) in \( K[x] \). So \( (x-a) \) divides \( gh + hf' = 1 \), which is a contradiction. \( \square \)

12.2. Example: Let \( p \) be a prime number and \( n \) be a natural number. Consider the polynomial \( f(x) = x^p^n - x \in \mathbb{F}_p[x] \). Then \( f'(x) = -1 \), so \( f \) and \( f' \) are relatively prime in \( \mathbb{F}_p[x] \). So \( f(x) \) cannot have repeated roots in any extension of \( \mathbb{F}_p \). In particular \( f(x) \) has \( p^n \) distinct roots in its splitting field.

12.3. Definition. Let \( F \) be a field of characteristic \( p \). Then \( \sigma : F \to F \), defined by \( \sigma(x) = x^p \), is a non-zero endomorphism of \( F \), since \((x+y)^p = x^p + y^p \). So \( \sigma \) is an isomorphism from \( F \) to some subfield \( \sigma(F) \) of \( F \). The map \( \sigma \) is called the Frobenius endomorphism.

12.4. Theorem (Existence and uniqueness of finite fields). For each prime number \( p \) and each natural number \( n \), there is a finite field \( \mathbb{F}_{p^n} \) of order \( p^n \). Any finite field is isomorphic to \( \mathbb{F}_{p^n} \) for some prime number \( p \) and natural number \( n \).

Proof. Let \( K \) be a finite field. Then the characteristic of \( K \) is a prime number, call it \( p \). So \( K \) is a finite extension of \( \mathbb{F}_p \). Let \( n = [K : \mathbb{F}_p] \). Then \( K \) has order \( q = p^n \). Since the multiplicative group \( K^* \) has order \( q-1 \), we have \( \alpha^{q-1} = 1 \) for all \( \alpha \in K^* \). So \( \alpha^q - \alpha = 0 \) for all \( \alpha \in K \). In other words, all the \( q \) elements of \( K \) are roots of the degree \( q \) polynomial \( f(x) = x^q - x \). In other words, \( f(x) \) splits in \( K \) as \( f(x) = \prod_{\alpha \in K} (x-a) \). Since \( f'(x) = -1 \) is relatively prime to \( f(x) \), the polynomial \( f(x) \) cannot have repeated root in any extension of \( \mathbb{F}_p \) so \( f(x) \) cannot split in any subfield of \( K \) (since \( K \) has only \( q \) elements !). It follows that \( K \) is a splitting field of \( f(x) \). This also suggests a way to construct a field of order \( q \).

Let \( F \) be a splitting field of \( f(x) \in \mathbb{F}_p[x] \). Note that Let \( \mathbb{F}_q \) be the set of all roots of \( f(x) \) in \( F \). Since \( f'(x) = -1 \), we saw that \( f(x) \) cannot have repeated roots in any extension, so \( \mathbb{F}_q \) has \( q \) elements. Let \( a, b \in \mathbb{F}_q \). Then \((a + b) \in \mathbb{F}_q \) and \( ab \in \mathbb{F}_q \) (since the Frobenius is an automorphism of \( \mathbb{F}_q \)). Also \((-a)^q = -a^q = -a \), so \( -a \in \mathbb{F}_q \). If \( a \neq 0 \), then \( a^q = a \) gives \( a^{-1} = a^{-q-1}a = a^{-q}a = (a^{-1})^q \), so \( a^{-1} \in \mathbb{F}_q \). So \( \mathbb{F}_q \subseteq F \) is already a field in which \( f \) splits, hence \( F = \mathbb{F}_q \) is the splitting field of \( f(x) \in \mathbb{F}_p[x] \). The uniqueness follows from the uniqueness of splitting field. \( \square \)

12.5. Definition. If \( d \) a natural number, let \( \Phi(d) \) be the set of integers \( x \) such that \( 1 \leq x \leq d \) and \( x \) is relatively prime to \( d \). Let \( \phi(d) \) be the number of elements in \( \Phi(d) \). Observe that \( d \Phi(n/d) \) is exactly the set of elements of \( \{1, 2, \ldots, n\} \) whose gcd with \( n \) is equal to \( d \). So

\[
\{1, 2, \ldots, n\} = \bigsqcup_{d \mid n} d \Phi(n/d).
\]
Counting both sides, we get

\[ n = \sum_{d|n} \phi(d). \]  

(3)

12.6. **Lemma.** Let \( H \) be a finite group of order \( n \). Suppose, for each divisor \( d \) of \( n \), the set \( \{ x \in H : x^d = 1 \} \) has at most \( d \) elements. Then \( H \) is cyclic.

**Proof.** Let \( d \) be a divisor of \( n \). Let \( H_d \) be the set of elements of \( H \) of order \( d \). If \( a \in H_d \), then \( (a) = \{1, a, \cdots, a^{d-1}\} \) already gives \( d \) elements in \( H \) satisfying the equation \( x^d = 1 \). So \( (a) \) must be the set of all elements satisfying \( x^d = 1 \), so \( H_d \subseteq (a) \), so \( |H_d| = \phi(d) \). It follows that \( |H_d| = 0 \) or \( |H_d| = \phi(d) \). But \( \sum_{d|n} |H_d| = n = \sum_{d|n} \phi(d) \). So we must have \( |H_d| = \phi(d) \) for all \( d \). In particular \( H_n \neq \emptyset \), so \( H \) has an element of order \( n \). \( \square \)

12.7. **Theorem.** The multiplicative group of a finite field is cyclic.

**Proof.** Let \( H \) be the multiplicative group of a finite field. Then \( H \) satisfies the hypothesis of 12.6 since a polynomial of degree \( d \) with coefficients in a field has at most \( d \) roots. \( \square \)
13. Seperability

13.1. Definition. Let $F$ be a field. Fix an algebraic closure $\bar{F}$ of $F$. Let $K/F$ be an extension. Let $a \in K$ and let $p(x) \in F[x]$ be a minimal polynomial of $a$. A root of $p$ in $\bar{F}$ is called a conjugate of $a$. So $a$ has at most $d = \deg(p)$ many conjugates. Say that $a$ is an separable element (over $F$) if $a$ has $d$ conjugates, or equivalently, if $p(x)$ has $d$ distinct roots, or equivalently, if $p(x)$ is separable. Call an algebraic extension $K/F$ separable if each $a \in K$ is separable.

13.2. Lemma. Any algebraic extension of a field of characteristic zero or any algebraic extension of a finite field is separable.

Proof. Let $K$ be any algebraic extension of a field $F$ of characteristic zero. Let $a \in K$. Then the minimal polynomial $p(x)$ of $a$ is irreducible, so $\deg(p)$ implies that $a$ is separable. So $K/F$ is a separable.

Let $K$ be any algebraic extension of $\mathbb{F}_p$. Let $a \in K$, then $\mathbb{F}_p(a)$ is a finite extension of $\mathbb{F}_p$, so $\mathbb{F}_p(a) \cong \mathbb{F}_{p^n}$ for some $n \geq 1$. So $a$ satisfies the polynomial $f(x) = x^{p^n} - x$ so the minimal polynomial $p(x)$ of $a$ over $\mathbb{F}_p$ is a factor of $f(x)$. Since $f(x)$ does not have any repeated root in $\mathbb{F}_p$, the minimal polynomial $p(x)$ does not have any repeated roots either. So $a$ is separable an separable element. Thus $K/\mathbb{F}_p$ is separable.

13.3. Example. A standard example of nonseparable extension is $\mathbb{F}_p(t) \subseteq \mathbb{F}_p(t^{1/p})$.

13.4. Lemma. Let $K/F$ be an extension and $a \in K$. Then $a$ is separable if and only if $a$ satisfies a polynomial $f(x) \in F[x]$ that has all distinct roots, i.e. that splits into distinct linear factors in $\bar{F}[x]$.

Proof. Let $p(x) \in F[x]$ be the minimal polynomial of $a$. If $f(a) = 0$, then $p(x)$ divides $f(x)$. So if $f(x)$ has distinct roots, then so does $p(x)$.

13.5. Definition. Let $K \supseteq F$ be an extension with $[K : F] = n$. Let $[K : F]_s$ be the number of embeddings $\sigma : K \to \bar{F}$ fixing $F$ pointwise (i.e. $\sigma$ restricted to $F$ is identity). This number is called the separable degree of the extension $K/F$.

13.6. Theorem. Let $K = F(a)$ be a finite simple extension of $a$. Let $p(x) \in F[x]$ be the minimal polynomial of $a$. Then there is a bijection between the set of roots of $p(x)$ and the set of embedding of $K$ in $\bar{F}$ fixing $F$. So the separable degree $[K : F]_s$ is equal to the number of distinct conjugates of $a$ in $K$. One has $[K : F]_s \leq \deg(p) = [K : F]$. The equality $[K : F]_s = [K : F]$ holds if and only if $a$ is a separable element.

Proof. Let $a_1, a_2, \ldots, a_r$ be the distinct conjugates of $a$, i.e. the roots of the minimal polynomial $p$. An embedding $\sigma : K \to \bar{F}$ sends $a$ to a conjugate of $a_i$ since $p(a) = 0$ implies $p(\sigma(a)) = 0$. Conversely, verify that, for each conjugate $a_i$, one gets an embedding of $K \to \bar{F}$ by sending $a$ to $a_i$. So the separable degree of $F(a)/F$ is equal to $r \leq \deg(p) = [K : F]$.

The equality $[K : F] = [K : F]_s$ holds if and only if $p$ has deg(p) many distinct roots, in other words, all distinct roots; that is, $a$ is separable.

13.7. Theorem. Let $K/F$ be an finite extension. Let $M$ be a field such that $K \supseteq M \supseteq F$.

(a) Then one has $[K : F]_s = [K : M]_s [M : F]_s$.

(b) One has $[K : F]_s \leq [K : F]$ and equality holds if and only if $K/F$ is separable.

(c) $K/F$ is separable if and only if $K/M$ and $M/F$ are separable.
Proof. (a) Fix an algebraic closure $E \supseteq M$. Then $E$ is also an algebraic closure of $F$; we write. We have a map

$$\text{res}_M : \{\text{Embeddings of } K \text{ in } E \text{ fixing } F\} \rightarrow \{\text{Embeddings of } M \text{ in } E \text{ fixing } F\}$$
given by $\text{res}_M(\lambda) = \lambda|_M$. Any embedding $\mu : M \rightarrow E$ can be extended to an embedding $\lambda : K \rightarrow E$ (by 11.6) and in $[K : M]_s$ many different ways. So the map $\text{res}_M$ is onto and the preimage of every element has size $[K : M]_s$. Part (a) follows.

(b) The inequality $[K : F]_s \leq [K : F]$ is proved by induction on $[K : F]$. Pick $a \in K \setminus F$ and let $M = F(a)$. Theorem 13.6 implies $[M : F]_s \leq [M : F]$. Since $[K : M] < [K : F]$, by induction we may assume $[K : M]_s \leq [K : M]$. Using part (a) we now get

$$[K : F]_s = [K : M]_s[M : F]_s \leq [K : M][M : F] = [K : F].$$

If $K/F$ is separable, then $[K : F] = [K : F]_s$ follows by similar induction.

Conversely, suppose $[K : F] = [K : F]_s$. We have to show that, for each $a \in K$, the minimal polynomial $p(x)$ of $a$ has degree strictly larger than or equal to the degree, one must have $[F(a) : F]_s = [F(a) : F]$. Now 13.6 implies that $a$ is separable.

(c) Suppose $K/F$ is separable. Since each $x \in M$ is also an element of $K$ the minimal polynomial of $x$ must have distinct roots, so $M/F$ is separable. Now let $y \in K$. The minimal polynomial of $y$ over $M$ is a factor of its minimal polynomial over $F$, so must have distinct roots, whence $K/M$ is separable too.

Conversely, If $K/M$ and $M/F$ are separable, then $[K : M]_s = [M : F]$ and $[M : F]_s = [M : F]$, so $[L : K]_s = [L : K]$ which, now implies $L/K$ is separable. \hfill $\Box$

13.8. **Theorem** (Primitive element theorem). If $K/F$ be a finite separable extension. Then there is an $\gamma \in K$ such that $K = F(\gamma)$.

*Proof.* If $F$ is finite then $K = F(\gamma)$ where $\gamma$ is any generator for the multiplicative group of $K$. So assume that $F$ is infinite. Let $F(\alpha, \beta)$ be a separable extension of degree $n$. Then there are $n$ distinct embeddings $\{\sigma_1, \cdots, \sigma_n\}$ of $F(\alpha, \beta)$ in $\bar{F}$. Consider the nonzero polynomial $P(x) = \prod_{i \neq j} (\sigma_i \alpha - \sigma_j \alpha + x(\sigma_i \beta - \sigma_j \beta))$. Since $F$ is an infinite field, there exists $c \in F$ such that $P(c) \neq 0$ which implies that $\gamma = (\alpha + c\beta)$ has $n$ distinct images under the $\sigma_i$, i.e. $\gamma$ has $n$ distinct conjugates, so $[F(\gamma) : F]_s = n$. So $[F(\gamma) : F] = n$ and $F(\gamma) = F(\alpha, \beta)$. \hfill $\Box$

13.9. **Corollary.** If $K$ is an separable extension of $F$ such that for every $\alpha \in K$, we have $[F(\alpha) : F] \leq n$. Then $[K : F] \leq n$.

*Proof.* Pick $\alpha$ so that $[F(\alpha) : F] = m$ is maximal. If $\beta$ is $K$ but not in $F(\alpha)$ then the extension $F(\alpha, \beta)/F$ has degree strictly larger than $m$ and is simple by the primitive element theorem. This contradicts the maximality of $m$; so $K = F(\alpha)$. \hfill $\Box$
14. Galois theory

14.1. Definition. Say that $K/F$ is a normal extension if $K$ is a splitting field of a collection of polynomials in $F[x]$, in other words, if every embedding of $K$ in $\bar{F}$ fixing $F$, is an automorphism of $F$.

14.2. Lemma. Let $K/F$ be an algebraic extension. The following are equivalent:

(a) $K/F$ is normal.
(b) every embedding of $K$ in $\bar{F}$ fixing $F$ is an automorphism of $K$.
(c) If $a \in K$, each conjugate of $a$ also belong to $K$.
(d) Every $a \in K$ satisfies a polynomial in $F[x]$ that splits into linear factors in $K[x]$.

Proof. The equivalence of (a) and (b) is contained in 11.10. An embedding of $K \in \bar{F}$ takes each $a \in K$ to some conjugate of $a$, hence the equivalence of (b) and (c).

Let $a \in K$ and let $p(x) \in F[x]$ be the minimal polynomial of $a$. Recall that the conjugates of $a$ are precisely the roots of $p(x)$. So if all the conjugates of $a$ are in $K$, then $p(x)$ splits into linear factor in $K[x]$, hence (c) implies (d). Conversely assume (d). Let $f(x) \in F[x]$ such that $f(a) = 0$ and $f$ splits into linear factors in $K[x]$. Now $p(x) \mid f(x)$, so $p(x)$ also splits into linear factors in $K[x]$, i.e., all the roots of $p(x)$ are in $K$. Thus (d) implies (c). □

14.3. Lemma. (a) A compositum of normal extensions is normal.
(b) An Intersection of normal extensions is normal.
(c) Suppose $F \subseteq M \subseteq K$ be fields. If $K/F$ is a normal, then so is $K/M$.

Proof. Let $\{K_i: i \in I\}$ be a collection of fields $F \subseteq K_i \subseteq K$ such that $K$ is the compositum of $\{K_i: i \in I\}$. Suppose each $K_i/F$ is normal. Let $\sigma : K \to \bar{F}$ be any embedding fixing $F$. Then $\sigma|_{K_i}$ is an embedding of $K_i$ in $\bar{F}$ so 11.10 implies that $\sigma|_{K_i}$ is an automorphism of $K_i$, that is, $\sigma(K_i) = K_i$ for each $i$. Since $K$ is generated by the $K_i$’s it follows that $\sigma(K) = K$. This proves (a). Part (b) and (c) are easier exercises. □

14.4. Definition. Let $K/F$ be an extension. We let $\text{Aut}(K/F)$ be the set of field automorphisms of $K$ fixing $F$ pointwise. Clearly, $\text{Aut}(K/F)$ is a group. Let $H$ be a subset of $\text{Aut}(K/F)$. Then we let $K^H$ denote the set of elements of $K$ that are fixed by each element of $H$. One verifies that $K^H$ is a subfield of $K$ containing $F$. We say that $K^H$ is the fixed field of $H$.

14.5. Lemma. Let $K/F$ be an finite extension. The following are equivalent:

(a) $K/F$ is normal and separable.
(b) $|\text{Aut}(K/F)| = [K : F]_s = [K : F]$.
(c) Each $a \in K$ satisfies a polynomial in $F[x]$ that splits into distinct linear factors in $K[x]$.

Proof. If $\tau$ is any embedding of $K$ in $\bar{F}$ fixing $F$, then $\{\tau \circ \sigma: \sigma \in \text{Aut}(K/F)\}$ gives $|\text{Aut}(K/F)|$ many distinct embeddings. Thus, one always has

$|\text{Aut}(K/F)| \leq [K : F]_s \leq [K : F]$.

The equality $[K : F]_s = [K : F]$ holds if and only if $K/F$ is separable (see 13.7) and the equality $|\text{Aut}(K/F)| = [K : F]_s$ holds if and only if $K/F$ is normal (see 11.10). This proves the equivalence of (a) and (b). Equivalence of (a) and (c) follows from 14.2 and 13.4. □
14.6. **Definition.** A finite extension $K/F$ is called **Galois**, if it satisfies the equivalent conditions of 14.5. If $K/F$ is a Galois extension, then the group $\text{Aut}(K/F)$ called the Galois group of $K/F$ and is denoted by $\text{Gal}(K/F)$.

14.7. **Lemma.** Let $K/F$ be a Galois extension. Let $M$ be a field such that $F \subseteq M \subseteq K$. Then $K/M$ is Galois and $M/F$ is separable.

**Proof.** Exercise.

14.8. **Lemma.** Let $K/F$ be a Galois extension with Galois group $G$. Then $K^G = F$.

**Proof.** Let $\alpha \in K^G$ and $\sigma$ be any embedding of $F(\alpha)$ in $\bar{F}$ fixing $F$. Then $\sigma$ extends to an embedding $\sigma_1 : K \rightarrow \bar{F}$. Any such embedding $\sigma_1$ must be an automorphism of $K$ fixing $F$, so $\sigma_1$ must fix $\alpha$. In other words $\sigma$ fixes $\alpha$. Thus $|F(\alpha) : F| = 1$, so $F(\alpha) = F$. □

14.9. **Lemma.** Let $K/F$ be a Galois extension with galois group $G$. Fix an algebraic closure $\bar{F}$ of $F$ containing $K$. Let $a \in K$. Then the orbit $G.a$ of $a$ under $G$ is equal to the set of all the conjugates of $a$ in $\bar{F}$. Let $G.a = \{a_1, \ldots, a_r\}$ and

$$p(x) = \prod_{j=1}^{r}(x - a_j).$$

Then $p(x) \in F[x]$ and is the minimal polynomial of $a$ over $F$.

**Proof.** If $\sigma \in G$, then $\sigma(a)$ and $a$ satisfies the same polynomials in $F[x]$, so $\sigma(a)$ is a conjugate of $a$. Conversely, let $b \in \bar{F}$ be a conjugate of $a$, then there exists an embedding $\sigma' : F(a) \rightarrow \bar{F}$ such that $\sigma'(a) = b$. Lemma 11.9 implies that $\sigma'$ extends to an embedding $\sigma : K \rightarrow \bar{F}$ fixing $F$. Since $K/F$ is normal, $\sigma \in G$. So $b = \sigma(a) \in G.a$.

Each $g \in G$ permutes the set $G.a = \{a_1, \ldots, a_r\}$. So $g(p) = p$, hence the coefficients of $p$ are in $K^G$. But $K^G = F$ by 14.8 So $p(x) \in F[x]$ and $p(a) = 0$. So $p(x)$ is a multiple of the minimal polynomial of $a$. On the other hand, each $a_j$ is a conjugate of $a$, so is a root of the minimal polynomial of $a$. Since $a_j$'s are distinct, $\prod_{j}(x - a_j)$ is a factor of the minimal polynomial of $a$. □

14.10. **Theorem** (Artin's theorem). Let $G$ be a finite group of automorphisms of $K$ of order $n$ and $F = K^G$ be the fixed field. Then $K/F$ is Galois of degree $n$ with Galois group $G$.

**Proof.** Let $a$ in $K$. Let $G.a = \{a_1, \ldots, a_r\}$ be the set of conjugates of $a$. By 14.9, $p(x) = \prod_{j=1}^{r}(x - a_j) \in F[x]$ is the minimal polynomial of $a$. Since $p(x)$ splits in $K[x]$ into distinct linear factors, 14.5 implies that $K/F$ is Galois.

One has $|F(a) : F| = \deg(p) \leq n$, so 13.9 implies that $|\text{Gal}(K/F)| = [K : F] \leq n$. On the other hand, clearly, $G \subseteq \text{Gal}(K/F)$ which already has order $n$. So $G = \text{Gal}(K/F)$. □

14.11. **Theorem** (Fundamental theorem of Galois theory). Let $L/F$ be a finite Galois extension with Galois group $G$. Then there is an inclusion reversing bijection between the subgroups of $G$ and the subfields of $L$ that contain $F$, given by

$$M \mapsto \text{Gal}(L/M), \text{ where } M \text{ is some subfield of } L \text{ containing } F.$$ This is called the Galois correspondence. The inverse correspondence is given by by $H \mapsto L^H$.

(b) Let $H$ be a subgroup of $G$. Then $L/L^H$ is Galois with galois group $H$.

(c) Let $F \subseteq M \subseteq L$. The extension $M/F$ is normal (Galois) if and only if $H = \text{Gal}(L/M)$ is normal in $G$ and in that case $\text{Gal}(M/F) = G/H$.
Proof. (a) Let $M$ be some field between $L$ and $F$. We already know $L/M$ is Galois. If $H = \text{Gal}(L/M)$, then $M = L^H$ by 14.8. Hence the injectivity of the correspondence $M \mapsto \text{Gal}(L/M)$. (note that this part of the theorem holds even for infinite extensions). The surjectivity of the correspondence as well as part (b) follows from Artin’s theorem.

(c) Suppose $M/F$ is normal. One verifies that there is a homomorphism $\text{res}_M : G = \text{Gal}(L/F) \to \text{Gal}(M/F)$ given by $\text{res}_M(\sigma) = \sigma|_M$ with kernel $H = \text{Gal}(L/M)$. So $H$ normal subgroup of $G$. Furthermore any automorphism of $M$ fixing $F$ extends to an embedding and hence an automorphism of $L$. So $\text{res}_M$ is onto and $\text{Gal}(M/F) = G/H$. Conversely, if $M$ is not a normal extension then there is an embedding $\lambda$ of $M$ into $L$ fixing $F$ such that $\lambda M \neq M$. Verify that $\text{Gal}(L/\lambda M) = \lambda \text{Gal}(L/M)\lambda^{-1}$. So $\text{Gal}(L/\lambda M)$ and $\text{Gal}(L/M)$ are conjugates and belong to distinct subfields $M$ and $\lambda M$, so they are not equal, showing that $\text{Gal}(L/M)$ is not normal.

14.12. Theorem (The normal basis theorem). If $L/K$ is a finite Galois extension and then there is an element $w$ in $L$ such that its images under $\text{Gal}(L/K)$ form a basis of $L/K$.

Proof. For a infinite field $K$ look at the polynomial $\det(\sigma_i^{-1}\sigma_j)$ as a polynomial function of the automorphisms $\sigma_1, \ldots, \sigma_n$ in $\text{Gal}(L/K)$. This polynomial is nonzero, so find an $w$ in $L$ with $\det(\sigma_i^{-1}\sigma_j(w)) \neq 0$. Now a relation $a_1\sigma_1(w) + \cdots + a_n\sigma_n(w) = 0$ with $a_i$ in $K$ implies $n$ linear equations by applying $\sigma_i^{-1}$ to it. Since $((\sigma_i^{-1}\sigma_j(w)))$ is invertible $a_i$ must all be zero. □