3. Let $\mathfrak{p}$ be a prime ideal of A. Show that $A_\mathfrak{p}$ has a unique maximal ideal, consisting of all elements a/s with $a \in \mathfrak{p}$ and $s \notin \mathfrak{p}$.

Proof. Let $\mathfrak{m} = \{a/s \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$. First, we will show that $\mathfrak{m}$ is proper. If $1 \in \mathfrak{m}$, then $a/s = 1/1$ for some $a \in \mathfrak{p}$, $s \notin \mathfrak{p}$, meaning $r(a-s) = 0$ for some $r \notin \mathfrak{p}$. But we know $a - s \notin \mathfrak{p}$, and thus $0 = r(a-s) \notin \mathfrak{p}$ (because the complement of $\mathfrak{p}$ is multiplicative), a contradiction. So $1 \notin \mathfrak{m}$, hence $\mathfrak{m}$ is proper.

Let $\mathfrak{a}$ be an ideal of $A_\mathfrak{p}$, but suppose that $\mathfrak{a} \not\subseteq \mathfrak{m}$. Then for some $a, s \notin \mathfrak{p}$ we have $a/s \in \mathfrak{a}$. But then $s/a \in \mathfrak{a}$ as well, meaning $1 \in \mathfrak{a}$ and hence $\mathfrak{a}$ is not proper. Therefore, $\mathfrak{m}$ contains every proper ideal of $A_\mathfrak{p}$, thus is maximal. □

4. Let A be a principal ring and S a multiplicative subset with $0 \notin S$. Show that $S^{-1}A$ is principal.

Proof. Let $\mathfrak{b}$ be an ideal of $S^{-1}A$, and define $\mathfrak{a} = \{a \mid a/s \in \mathfrak{b} \text{ for some } s \in S\}$. We will show $\mathfrak{a}$ is an ideal of A. Let $a \in \mathfrak{a}$ and $c \in A$. There is some $s \in S$ such that $a/s \in \mathfrak{b}$, so $\frac{a}{s}\frac{c}{1} = \frac{ac}{s} \in \mathfrak{b}$, since $\mathfrak{b}$ is an ideal. Thus, $ac \in \mathfrak{a}$, so $\mathfrak{a}$ is closed under multiplication by A. Next, let $a, b \in \mathfrak{a}$, so that $a/s, b/t \in \mathfrak{b}$ for some $s, t \in S$. Then $\frac{a}{s} - \frac{t}{s}\frac{y}{t} = \frac{x-y}{s} \in \mathfrak{b}$, so $x - y \in \mathfrak{a}$. Clearly, $0/1 \in \mathfrak{b}$, so $\mathfrak{a}$ is an ideal.

Since A is principal, $\mathfrak{a} = (k)$ for some $k \in A$. Thus, $\mathfrak{b} = \{\frac{a}{s} \cdot \frac{k}{1} \mid a/s \in S^{-1}A\} = (k/1)$ is principal. Finally, since $0 \notin S$, we know $S^{-1}A \neq \{0\}$. Thus $S^{-1}A$ is principal. □

5. Let A be a factorial ring and S a multiplicative subset of $0 \notin S$. Show that $S^{-1}A$ is factorial, and that the prime elements of $S^{-1}A$ are of the form up with primes p of A such that $(p) \cap S$ is empty, and units u in $S^{-1}A$.

Proof. Note that, since A is an integral domain and $0 \notin S$, $\frac{x}{s} = \frac{y}{t}$ if and only if $xt = ys$. Also, since A is a UFD, irreducibles are prime. Finally, if every element of an integral domain R factors as a product of irreducibles *and* all irreducibles in R are prime, then R is a UFD. (Given two factorizations $\prod_i^m p_i$ and $\prod_j^n q_i$ with $m \leq n$, we can relabel the factors so that $p_i \mid q_i$ for each i. But q_i is irreducible, so $q_j = u_i p_i$ for some unit u_i. If we had $m < n$, then dividing through by $\prod_i^m p_i$s would leave us with a product of irreducibles equal to 1, a contradiction.)

Let $p \in A$ be irreducible. Suppose first that $(p) \cap S \neq \emptyset$, so that $s = pa$ for some $s \in S$, $a \in A$. Then $\frac{p}{1}\frac{a}{s} = \frac{pa}{s} = \frac{s}{s} = \frac{1}{s}$, hence $p/1$ is a unit. Conversely, if $p/1$ is a unit then $\frac{p}{1}\frac{a}{s} = \frac{1}{1}$ for some $a \in A, s \in S$. This must mean $pa = s$, so that $(p) \cap S \neq \emptyset$. So $(p) \cap S \neq \emptyset$ if and only if $p/1$ is a unit.

Next, suppose $(p) \cap S = \emptyset$, where again $p \in A$ is irreducible. Suppose $\frac{p}{1} = \frac{a}{s}\frac{b}{t}$. Then $pst = xy$, so p divides either x or y. Assuming $p \mid x$, we have $x = px'$ so $\frac{x'}{s}\frac{y}{t} = 1$, hence $\frac{y}{t}$ is a unit. Since $(p) \cap S = \emptyset$, we know $p/1$ cannot be a unit. Therefore, it is irreducible. So if $(p) \cap S = \emptyset$ then $p/1$ is irreducible.

We can factor any $a \in A$ as $a = \prod_i q_i \prod_i p_i$, where $(q_i) \cap S \neq \emptyset$ and $(p_i) \cap S = \emptyset$ for each i. Thus, for any $s \in S$, a/s has a factorization into units, namely

$$a/s = \left(\frac{1}{s}\prod_i \frac{q_i}{1}\right)\prod_i \frac{p_i}{1}$$

where the left-hand factor is a unit and the right-hand factor is the product of all irreducibles p in a given factorization of a for which $(p) \cap S = \emptyset$. This also means that, if a/s is irreducible, then $a/s = u(p/1)$, where $u \in S^{-1}A$ is a unit and p is an irreducible such that $(p) \cap S = \emptyset$.

Finally, let $u(p/1)$ be irreducible, and suppose it divides $\frac{a}{s}\frac{b}{t}$. We wish to show that $u(p/1)$ divides one of $\frac{a}{s}$ or $\frac{b}{t}$, completing the proof. We may assume $u = 1$ since, in any commutative ring, an element α divides another β if and only if $\alpha \cdot u$ divides β for all units u. So $\frac{p}{1}\frac{c}{r} = \frac{a}{s}\frac{b}{t}$ for some $r \in S, c \in A$, giving

$$pstc = rab.$$

Since p is prime in A but divides no element of S, we must have $p \mid a$ or $p \mid b$. If WLOG $p \mid a$, then $pd = a$ for some $d \in A$. Thus, $\frac{p}{1}\frac{d}{s} = \frac{a}{s}$, so $\frac{p}{1} \mid \frac{a}{s}$. Therefore, $u(p/1)$ is prime, and so $S^{-1}A$ is a UFD. □

6. Let A be a factorial ring and p a prime element. Show that the local ring $A_{(p)}$ is principal.

Proof. Let $\mathfrak{a} \subseteq A_{(p)}$ be an ideal. If $a/s \in \mathfrak{a}$, then $p^k \mid\mid a$ for some j. So a factors as $p^j p_1 \cdots p_n$ where $p \nmid p_i$ for all i. Hence $\frac{1}{p_1 \cdots p_n} \in A_{(p)}$, meaning that $p^j/1 \in \mathfrak{a}$. If we let k be the minimum exponent such that $p^k/1 \in \mathfrak{a}$, then it is clear from this discussion that $\mathfrak{a} = (p^k/1)$. $\square$

3. Let R be an entire ring containing a field k as a subring. Suppose that R is a finite dimensional vector space over k under the ring multiplication. Show that R is a field.

Proof. Let $x \in R$ be nonzero. There exists some n such that $c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = 0$ for some $c_0, c_1, \ldots, c_n \in k$ (not all zero); otherwise, the set $\{x^k : k \in \mathbb{N}\}$ forms an infinite linearly independent set over k, contradicting that R is finite dimensional over k. Also, $n > 1$ because $x \neq 0$. Let m be the minimum index such that $c_m \neq 0$. Then

$$c_m x^m + \cdots c_n x^n = x^m(c_m + c_{m+1}x + \cdots + c_n x^{n-m}) = 0.$$

Because R is entire, one of the two factors must be 0. But $x^m \neq 0$, else x is a zero divisor. So the righthand factor is 0. This gives us

$$x\left(-\frac{c_{m+1}}{c_m} - \frac{c_{m+2}}{c_m}x - \cdots - \frac{c_n}{c_m}x^{n-m-1}\right) = -\frac{c_{m+1}}{c_m}x - \frac{c_{m+2}}{c_m}x^2 - \cdots - \frac{c_n}{c_m}x^{n-m} = 1$$

therefore $x^{-1} = -\frac{c_{m+1}}{c_m} - \frac{c_{m+2}}{c_m}x - \cdots - \frac{c_n}{c_m}x^{n-m-1}$, so R is a field. $\square$

4. **Direct Sums**

(a) Prove in detail that the conditions given in Proposition 3.2 for a sequence to split are equivalent. Show that a sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ splits if and only if there exists a submodule N of M such that M is equal to the direct sum $\operatorname{Im} f \oplus N$, and that if this is the case, then N is isomorphic to M''. Complete all the details of the proof of Proposition 3.2.

Proof. First, we wish to show that, if the above sequence is exact, then the following are equivalent:

(1) There exists a homomorphism $\varphi : M'' \to M$ such that $g \circ \varphi = \mathrm{id}$.

(2) There exists a homomorphism $\psi : M \to M'$ such that $\psi \circ f = \mathrm{id}$.

Suppose that such a φ exists, and let $m \in M$. Letting $m'' = g(m)$, we have $g(m - \varphi(m'')) = g(m) - g \circ \varphi(m'') = 0$, thus $m - \varphi(m'') \in \operatorname{Ker}(g)$. So $m = (m - \varphi(m'')) + \varphi(m'')$, meaning

$$M = \operatorname{Ker} g + \operatorname{Im} \varphi.$$

If $x \in \operatorname{Ker} g \cap \operatorname{Im} \varphi$, then $x = \varphi(m'')$ for some $m'' \in M''$; but then $g(x) = g \circ \varphi(m'') = m'' = 0$, hence $x = g(0) = 0$. Thus, the sum is direct. Since $M' \cong \operatorname{Im} f = \operatorname{Ker} g$ and $M'' \cong \operatorname{Im} \varphi$, we have

$$M \cong M' \oplus M''.$$

Next, suppose that such a ψ exists, and let $m \in M$. Letting $m' = \psi(m)$, we have $\psi(m - f(m')) = \psi(m) - \psi \circ f(m') = m' - m' = 0$, so $m - f(m') \in \operatorname{Ker} \psi$. We have $m = f(m') + (m - f(m'))$, thus

$$M = \operatorname{Im} f + \operatorname{Ker} \psi.$$

Again, if $x \in \operatorname{Im} f \cap \operatorname{Ker} \psi$, then $x = f(m')$ for some $m' \in M'$, and so $\psi(x) = \psi \circ f(m') = m' = 0$. Therefore, $x = f(0) = 0$, so the sum is direct.

We have just proven that (1) and (2) both imply that the sequence splits. Now, suppose the sequence splits, i.e. $M = M' \oplus M''$ where f is the inclusion of M' and g is projection onto M''. Taking ψ to be projection of M onto M' and φ to be inclusion of M'' into M we have

$g \circ \varphi = \psi \circ f = \text{id}$; hence (1) and (2) are both equivalent to the sequence slitting, and thus equivalent to each other.

Since f is the inclusion of M', we know that $M = \operatorname{Im} f \oplus N$ for some submodule N. But $\operatorname{Im} f \cong \operatorname{Ker} g$, therefore

$$M'' \cong M/\operatorname{Ker} g = M/\operatorname{Im} f \cong N$$

where the last equivalence follows from the fact that $0 \to A \to A \oplus B \to B \to 0$ is exact for any modules A and B, so $(A \oplus B)/A \cong B$ (we are taking $A = \operatorname{Im} f$ and $B = N$).

□

(b) Let E and E_i $(i = 1, \dots, m)$ be modules over a ring. Let $\varphi_i : E_i \to E$ and $\psi_i : E \to E_i$ be homomorphisms having the following properties:

$$\psi_i \circ \varphi_i = \text{id}, \qquad \psi_i \circ \varphi_j = 0 \qquad \text{if } i \neq j$$

$$\sum_{i=1}^{m} \varphi_i \circ \psi_i = \text{id}$$

Show that the map $x \mapsto (\psi_1 x, \dots, \psi_m x)$ is an isomorphism of E onto the direct product of the E_i, and that the map $(x_1, \dots, x_m) \mapsto \varphi_1 x_1 + \cdots + \varphi_m x_m$ is an isomorphism of this direct product onto E. Conversely, if E is equal to a direct product (or direct sum) of submodules E_i, if we let φ_i be the inclusion of E_i in E, and ψ_i the projection of E on E_i, then these maps satisfy the above-mentioned properties.

Proof. Let $\psi : E \to \prod E_i$ be the first map and $\varphi : \prod E_i \to E$ be the second. Then

$$\begin{aligned}
\psi \circ \varphi(x_1, \dots, x_m) &= \psi(\varphi_1(x_1) + \cdots + \varphi(x_m)) \\
&= \psi(\varphi_1 x_1) + \cdots + \psi(\varphi x_m) \\
&= (\psi_1 \varphi_1 x_1, \dots, \psi_1 \varphi_m x) + \cdots + (\psi_m \varphi_1 x, \dots, \psi_m \varphi_m x) \\
&= (x_1, 0, \dots, 0) + \cdots + (0, \dots, 0, x_m) \\
&= (x_1, \dots, x_m) \\
\varphi \circ \psi(x) &= \varphi(\psi_1 x, \dots, \psi_m x) \\
&= \varphi_1 \psi_1 x + \cdots + \varphi_m \psi_m x \\
&= \sum_{i=1}^{m} \varphi_i \circ \psi_i(x) \\
&= x
\end{aligned}$$

so ψ and φ are inverses of each other, thus both isomorphisms.

Next, assume E is a direct product of submodules E_i, φ_i is the inclusion of E_i, and ψ is the projection onto E_i. Then

$$\psi_i \circ \varphi_j(x) = \psi_i((0, \dots, 0, x, 0, \dots, 0))$$

is x if $i = j$ and 0 otherwise, so the first two properties are satisfied. Also,

$$\sum_{1}^{m} \varphi_i \circ \psi_i(x_1, \dots, x_m) = \sum_{1}^{m} \psi_i(x_i) = \sum_{1}^{m} (0, \dots, 0, x_i, 0, \dots, 0) = (x_1, \dots, x_m)$$

so the last property is satisfied. □

5. Let A be an additive subgroup of Euclidean space $\mathbf{R}^n$, and assume that in every bounded region of space, there is only a finite number of elements of A. Show that A is a free abelian group on $\leq n$ generators.

Proof. Let $\{v_1, \dots, v_m\}$ be a maximal $\mathbf{R}$-linearly independent set of elements from A (if $A = \{0\}$, take the empty set; otherwise, add linearly independent vectors until no new elements from A can be added). We may assume that m is the largest number for which such a set exists; this is possible because all such sets have size $\leq n$, hence some must have a maximum size. We will induct on m. Clearly, if $m = 0$ then $A = 0$, hence is free on 0 generators.

Let $A_0 = A \cap \operatorname{span}\{v_1, \dots, v_{m-1}\}$. Then $\{v_1, \dots, v_{m-1}\}$ is a maximal linearly independent subset of A_0, so by induction A_0 is free on $\{u_1, \dots, u_k\}$ for some $k \leq m-1$. However, the vector space spanned by $\{u_1, \dots, u_k\}$ contains $\{v_1, \dots, v_{m-1}\}$, thus we must have $m-1 \leq k$ as well. So $k = m-1$.

Let $S = A \cap \{a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_m v_m \mid 0 \leq a_i < 1 \text{ for } 1 \leq i \leq m-1, 0 \leq a_m \leq 1\}$. By the triangle inequality, S is bounded by $|u_1| + \cdots + |u_{m-1}| + |v_m|$, hence is finite. Also, every element of S has a unique representation of the given form, because $\{u_1, \dots, u_{m-1}, v_m\}$ is linearly independent - if v_m were in the span of the u_is, then the $\operatorname{span}\{u_1, \dots, u_{m-1}\}$ would contain $\operatorname{span}\{v_1, \dots, v_m\}$, contradicting that this latter set is linearly independent. So there is some $v'_m \in S$ which has a minimal but nonzero coefficient a_m when expanded in this way (we know this is well-defined because these expansions are unique and S is finite).

Let $B = \{u_1, \dots, u_{m-1}, v'_m\}$. B is linearly independent because $\{u_1, \dots, u_{m-1}\}$ is, and due to the uniqueness of the representations we just discussed, v'_m is not a linear combination of the u_is. Also, B spans A over $\mathbf{R}$: if there were some $v \in A \setminus \operatorname{span}(B)$ then v would be linearly independent of B, meaning that $\{u_1, \dots, u_{m-1}, v'_m, v\}$ is a linearly independent set, contradicting that m is the largest possible size of a linearly independent set in A.

Let $v \in A$. Then v can be expressed as a linear combination $b_1u_1 + \cdots + b_{m-1}u_{m-1} + b_m v'_m$. Letting $v'_m = a_1u_1 + \cdots + a_{m-1}u_{m-1} + a_m v_m$ be the expansion of v'_m, this gives

$$v = (b_1 + b_m a_1)u_1 + \cdots + (b_{m-1} + b_m a_{m-1})u_{m-1} + (b_m a_m)v_m.$$

Let $c_m = \lfloor a_m \rfloor$. Then the coefficient of v_m in $v - c_m v'_m$ is $(a_m - c_m)b_m$, which satisfies $0 \leq (a_m - c_m)b_m < b_m$ since $0 \leq a_m - c_m < 1$. Next, for each $i = 1, \dots, m-1$ let c_i be the floor of the coefficient of u_i in $v - c_m v'_m$. Then

$$v' = v - c_1u_1 - \cdots - c_{m-1}u_{m-1} - c_m v'_m$$

is in S. Since the coefficient of v_m is less than that in the expansion of v'_m, we know it must be 0. Therefore, v' is a $\mathbf{Z}$-linear combination of $\{u_1, \dots, u_{m-1}\}$. But also, $w' = c_1u_1 + \cdots + c_{m-1}u_{m-1} + c_m v'_m$ is in the span of $\{u_1, \dots, u_{m-1}, v'_m\}$. Thus, $v = v' + w \in \operatorname{span}\{u_1, \dots, u_{m-1}, v'_m\}$. So this set generates A. Since it is linearly independent, A is free on this set, and we have already explained that $m \leq n$. $\square$

6. Let G be a finite group operating on a finite set S. For $w \in S$, denote $1 \cdot w$ by $[w]$, so that we have the direct sum

$$\mathbf{Z}\langle S \rangle = \sum_{w \in S} \mathbf{Z}[w].$$

Define an action of G on $\mathbf{Z}\langle S \rangle$ by defining $\sigma[w] = [\sigma w]$ (for $w \in S$), and extending σ to $\mathbf{Z}\langle S \rangle$ by linearity. Let M be a subgroup of $\mathbf{Z}\langle S \rangle$ of rank $\#[S]$. Show that M has a $\mathbf{Z}$-basis $\{y_w\}_{w \in S}$ such that $\sigma y_w = y_{\sigma w}$ for all $w \in S$.

This exercise, as presently worded, appears to be false. It seems the intended exercise should add the condition that M is invariant under G, and relax the conclusion to say that M contains a submodule M' of full rank in M that is also G-invariant and has such a $\mathbf{Z}$-basis. Unfortunately, I can't seem to solve any version of the statement, true or false.