1. (VIII.4.1) Let $R$ be a commutative ring with identity and $I$ a finitely generated ideal of $R$. Let $C$ be a submodule of an $R$-module $A$. Assume that for each $r \in I$ there exists a positive integer $m$ (depending on $r$) such that $r^m A \subset C$. Show that for some integer $n$, $I^n A \subset C$.

**Answer:** Suppose $I$ is generated by $\{r_1, \ldots, r_k\} \subseteq R$ and $r_i^n A \subset C$. Let $n := n_1 + \cdots + n_k - k + 1$. Then $I^n$ is generated by $\{r_1^{\ell_1} \cdots r_k^{\ell_k} \mid \ell_1, \ldots, \ell_k \in \mathbb{N}, \ell_1 + \cdots + \ell_k = n\}$. Each generator $r_1^{\ell_1} \cdots r_k^{\ell_k}$ of $I^n$ satisfies that $r_i^{\ell_i} \geq n_i$ for some $i$. Therefore $r_1^{\ell_1} \cdots r_k^{\ell_k} A \subset C$. Hence $I^n A \subset C$.

2. (VIII.4.8) Let $R$ be a commutative Noetherian ring with identity and let $Q_1 \cap \cdots \cap Q_n = 0$ be a reduced primary decomposition of the ideal 0 of $R$ with $Q_i$ belonging to the prime ideal $P_i$. Then $P_1 \cup P_2 \cup \cdots \cup P_n$ is the set of zero divisors in $R$.

**Answer:** Let $S$ be the set of zero divisors of $R$.

1. If $r \in P_i$, there is $m \in \mathbb{Z}^+$ such that $r^m \in Q_i$. Let $r' \in \left( \bigcap_{j \neq i} Q_j \right) \setminus \{0\}$. Then $r^m r' \in Q_1 \cap \cdots \cap Q_n = 0$. So $r \in S$. Therefore, $P_1 \cup P_2 \cup \cdots \cup P_n \subseteq S$.

2. If $r \in S$, then $rr' = 0$ for some $r' \in R \setminus \{0\}$. Then $r' \not\in Q_i$ for some $i$, as $0 = Q_1 \cap \cdots \cap Q_n$ is the reduced primary decomposition of ideal 0. Since $Q_i$ is a primary ideal and $rr' \in Q_i$, $r' \in Q_i$ for some $t \in \mathbb{Z}^+$ and thus $r \in \text{Rad}(Q_i) = P_i$. Therefore, $S \subseteq P_1 \cup P_2 \cup \cdots \cup P_n$.

3. (VIII.5.6) If $S$ is an integral extension ring of $R$, then $S[x_1, \ldots, x_n]$ is an integral extension ring of $R[x_1, \ldots, x_n]$.

**Answer:** $S$ being an integral extension ring of $R$ if and only if the ring $S \geq R$ and $S$ is a finitely generated $R$-module. Suppose $S = \sum_{i=1}^m s_i R$. Then $S[x_1, \ldots, x_n] = \sum_{i=1}^m s_i R[x_1, \ldots, x_n]$. So the ring $S[x_1, \ldots, x_n] \supseteq R[x_1, \ldots, x_n]$ and $S[x_1, \ldots, x_n]$ is a finitely generated $R[x_1, \ldots, x_n]$-module. Therefore, $S[x_1, \ldots, x_n]$ is an integral extension ring of $R[x_1, \ldots, x_n]$.

4. (VIII.6.1) The ideal generated by 3 and $1 + \sqrt{5}i$ in the integral domain $\mathbb{Z}[\sqrt{5}i]$ is invertible.

**Answer:** Let $R := \mathbb{Z}[\sqrt{5}i]$. Let $\langle a_1, \ldots, a_n \rangle$ denote the $R$-module generated by $a_1, \ldots, a_n$. The fractional ideal $\langle 3, 1 + \sqrt{5}i \rangle^{-1} = \langle 3 \rangle^{-1} \cap \langle 1 + \sqrt{5}i \rangle^{-1} = \langle 1, 1 - \sqrt{5}i \rangle$. We have $\langle 3, 1 + \sqrt{5}i \rangle \langle 1, 1 - \sqrt{5}i \rangle = \langle 3, 1 - \sqrt{5}i, 1 + \sqrt{5}i, 2 \rangle = \langle 1 \rangle = R$. Thus $\langle 3, 1 + \sqrt{5}i \rangle$ is invertible.

**Answer:** Alternatively, we may show that $\mathbb{Z}[\sqrt{5}i]$ is a Dedekind domain, i.e., $\mathbb{Z}[\sqrt{5}i]$ is Noetherian, integrally closed, and every nonzero prime ideal is maximal.
5. (VIII.6.7) If $S$ is a multiplicative subset of a Dedekind domain $R$ (with $1_R \in S$, $0 \notin S$), then $S^{-1}R$ is a Dedekind domain.

**Answer:** Every proper ideal of $S^{-1}R$ is of the form $S^{-1}I$ for $I \triangleleft R$ and $S \cap I = \emptyset$. Since $R$ is Dedekind, $I$ is invertible. We have $II^{-1} = R$. Now $S^{-1}(I^{-1})$ is a fractional ideal of $S^{-1}R$, and $S^{-1}I \cdot S^{-1}I^{-1} = S^{-1}(II^{-1}) = S^{-1}R$. So $S^{-1}I$ is invertible in $S^{-1}R$. Therefore, $S^{-1}R$ is a Dedekind domain.

6. (V.1.1) Let $F$ be an extension field of $K$.

(a) \([F : K] = 1\) if and only if $F = K$.

**Answer:** $[F : K] = 1$ iff $F$ is a dimension 1 vector space over $K$, iff \(\{1\}\) is a basis of $K$, iff $F = K$.

(b) If $[F : K]$ is prime, then there are no intermediate fields between $F$ and $K$.

**Answer:** If $p = [F : K]$ is prime, then for $F \geq E \geq K$ we have $p = [F : E][E : K]$. Therefore, either $[F : E] = 1$ so that $E = F$, or $[E : K] = 1$ so that $E = K$.

(c) If $u \in F$ has degree $n$ over $K$, then $n$ divides $[F : K]$.

**Answer:** $F \geq K(v) \geq K$. So $[F : K] = [F : K(v)][K(v) : K] = n[F : K(v)]$ is divisible by $n$.

7. (V.1.14)

(a) If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, find $[F : \mathbb{Q}]$ and a basis of $F$ over $\mathbb{Q}$.

**Answer:** $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$. A basis of $F$ over $\mathbb{Q}$ is \(\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}\).

(b) Do the same for $F = \mathbb{Q}(i, \sqrt{3}, \omega)$, where $i = \sqrt{-1} \in \mathbb{C}$, and $\omega$ is a complex (nonreal) cube root of 1.

**Answer:** $x^3 - 1 = (x - 1)(x + \frac{1}{2} - i\frac{\sqrt{3}}{2})(x + \frac{1}{2} + i\frac{\sqrt{3}}{2})$ is a product of linear factors in $\mathbb{Q}(i, \sqrt{3})[x]$. Thus $\omega \in \mathbb{Q}(i, \sqrt{3})$. Therefore,

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(i, \sqrt{3})][\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 1 \cdot 2 \cdot 2 = 4.$$  

A basis of $F$ over $\mathbb{Q}$ is \(\{1, i, \sqrt{3}, \sqrt{3}i\}\).

8. (V.1.16) In the field $\mathbb{C}$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces over $\mathbb{Q}$, but not as fields.

**Answer:** The map $a + bi \mapsto a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$ defines an isomorphism of vector spaces over $\mathbb{Q}$ between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$.

If there is a field isomorphism $\phi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$, then $-1 = -\phi(1) = \phi(-1) = \phi(i^2) = \phi(i)^2$. This is impossible.