Problem 1. Let $R = F[x_1, \ldots, x_n]$ be a polynomial ring over a field $F$, and $M$ be a finitely generated $R$-module, and $f : M \to M$ be a surjective (i.e., onto) $R$-module homomorphism. Show that $f$ is a surjection.

Solution: We need to show that $\ker(f) = \ker(f^2) = \ker(f^3) = \ldots = (0)$. Assume the contrary. Choose an $0 \neq m \in M$ such that $m \in \ker(f)$, i.e., $f(m) = 0$.

Denote the $n$th iterate of $f$ by $f^n : M \to M$. Since $M$ is finitely generated, it is Noetherian, and the ascending sequence of submodules

$$\ker(f) \subset \ker(f^2) \subset \ker(f^3) \subset \ldots$$

has to terminate. Suppose $\ker(f^n) = \ker(f^{n+1})$. Since $f$ is surjective, so is $f^n$. Hence, there exists an $m' \in M$ such that $f^n(m') = m$. Now $f^{n+1}(m') = f(m) = 0$, so $m'$ lies in $\ker(f^{n+1})$ but not in $\ker(f^n)$, a contradiction.

Problem 2. Let $I = (x, y) \subseteq \mathbb{Q}[x, y]$ be the ideal generated by the variables $x$ and $y$. Here, as usual, $\mathbb{Q}[x, y]$ denotes the ring of polynomials in two variables with rational coefficients. All references to Gröbner bases below are with respect to the lexicographic monomial order in $\mathbb{Q}[x, y]$, with $x > y$.

(a) Exhibit two polynomials, $f_1, f_2 \in I$ such that $(f_1, f_2) = I$ but $\{f_1, f_2\}$ is not a Gröbner basis of $I$.

(b) Exhibit two monic polynomials, $f_3, f_4 \in I$ such that $\{f_3, f_4\}$ is a Gröbner basis of $I$ but not a minimal Gröbner basis. Here “monic” means that the leading term in the lexicographic order appears with coefficient 1.

(c) Exhibit two monic polynomials, $f_5, f_6 \in I$ such that $\{f_5, f_6\}$ is a minimal Gröbner basis for $I$ but not a reduced Gröbner basis.

Solution: (a) One can take, e.g., $f_1 = x$ and $f_2 = x + y$. The polynomials clearly generate $I$. However, the ideal $(x)$ generated by their leading monomials, does not contain $y = \text{LM}(y)$. This shows that $f_1$ and $f_2$ do not form a Gröbner basis for $I$.

(b) Such $f_3$ and $f_4$ do not exist. Apologies for not being more explicit about this possibility in the statement of the problem.

More generally,

Claim: Let $F$ be a field and $F[x_1, \ldots, x_n]$ be a polynomial ring in $n$ variables. Suppose an ideal $I \subseteq F[x_1, \ldots, x_n]$ has a minimal Gröbner basis $G = \{g_1, \ldots, g_r\}$. Then every Gröbner basis $H = \{h_1, \ldots, h_r\}$ of $I$ consisting of $r$ elements is minimal, as long as $h_1, \ldots, h_r$ are monic.

Proof: Assume the contrary: $H$ is not minimal. Then $\text{LM}(h_i)$ divides $\text{LM}(h_j)$ for some $i \neq j$, say, for $i = 1$ and $j = r$. We can now throw out $h_r$; the remaining polynomials $h_1, \ldots, h_{r-1}$ form a Gröbner basis, because

$$(\text{LM}(h_1), \ldots, \text{LM}(h_{r-1})) = (\text{LM}(h_1), \ldots, \text{LM}(h_{r-1}), \text{LM}(h_r)) = (\text{LM}(f) \mid f \in I).$$
If this Gröbner basis is not minimal proceed to remove further elements in the same manner, until we arrive at a minimal Gröbner basis of $I$, say (after renumbering) $H' = \{h_1, \ldots, h_d\}$ for some $d \leq r - 1$. Thus $I$ has two minimal Gröbner basis, $G$ with $r$ elements and $H'$ with $d \leq r - 1$ elements. But any two minimal bases for $I$ should have the same number of elements, a contradiction.

(c) Take, e.g., $f_5 = x + y$ and $f_6 = y$. This is minimal, because $\text{LM}(f_5) = x$ and $\text{LM}(f_6) = y$ do not divide each other, but it is not reduced, because $f_6$ has a term (namely, $y$) which is divisible by $\text{LM}(f_6)$.

**Problem 3.** Let $I$ be the ideal of $\mathbb{Q}[x, y]$ generated by the polynomials
\[ f_1 = x^2 y^2 - xy \text{ and } f_2 = xy^3 + y^2. \]
Find a Gröbner basis of $I$ with respect to the lexicographic monomial order, where $x > y$ (same monomial order as in Problem 2).

**Solution:** Compute the $S$-polynomial:
\[ f_3 = S(f_1, f_2) = yf_1 - xf_2 = -2xy^2. \]
Thus $I$ contains $-f_1 - \frac{1}{2}xf_3 = xy$ and $f_2 + \frac{1}{2}yf_3 = y^2$.

Claim: $I = (xy, y^2)$.

We just showed that $xy$ and $y^2$ lie in $I$; hence, $(xy, y^2) \subset I$. On the other hand, clearly both $f_1$ and $f_2$ lie in $(xy, y^2)$; hence, $I \subset (xy, y^2)$. This proves the claim.

Finally, $xy$ and $y^2$ form a Gröbner basis of $I$ by Buchberger’s criterion, since $S(xy, y^2) = y(xy) - x(y^2) = 0$.

**Problem 4.** Let $R$ be an integral domain.

(a) Let $S \subset R$ be a multiplicatively closed subset, such that $0 \notin S$ but $1 \in S$. Show that $S^{-1}R$ can be identified with a subring of the field of fractions $F = (R \setminus \{0\})^{-1}R$. That is, the map $f: S^{-1}R \to F$ taking $a/s$ in $S^{-1}R$ to $a/s$ in $F$ is well-defined and injective.

(b) As usual, if $M$ is a maximal ideal of $R$, we will denote by $R_M$ the local ring $S^{-1}R$, where $S = R \setminus M$. Show that
\[ R = \cap_{M \subset R} R_M, \]
where the intersection is taken inside $F$, over all maximal ideals $M$ of $R$.

**Solution:** (a) Assume $f(a/s) = 0$ in $F$ for some $a \in R$ and $s \in S$. That is, $a/s = 0/1$ in $F$. Then there exists a $u \in R \setminus \{0\}$ such that $(a \cdot 1 - s \cdot 0)u = 0$ in $R$. In other words, $au = 0$ in $R$. Since $R$ is an integral domain and $u \neq 0$, we conclude that $a = 0$, as desired.

(b) The inclusion $R \subset \cap_{M \subset R} R_M$ is clear.

To prove the opposite inclusion, suppose some $\alpha \in F$ lies in $\cap_{M \subset R} R_M$. Then for every maximal ideal $M$ in $R$ there is an element $s_M \in R \setminus M$ such that $s_M \alpha \in R$. 


Our goal is to show that $\alpha \in R$ or equivalently, that $1 \in I$, where $I \subset R$ is the conductor ideal, consisting of elements $a \in R$ such that $a\alpha \in R$. (Check that $I$ is an ideal of $R$!)

The above argument shows that $s_M \in I$ for every maximal ideal $M \subset R$. Thus $I$ does not lie in any maximal ideal $M$ of $R$. This shows that $I = R$ and thus $1 \in I$, as desired.

**Problem 5.** Let $F$ be a field. Show that the polynomial ring $R = F[x]$ is integrally closed in its field of fractions $E = F(x)$. That is, if $f \in E$ is integral over $R$, then $f \in R$.

**Solution:** Assume $f = p(x)/q(x)$ is integral over $R$, where $p(x)$ and $q(x)$ have no common factors of degree $\geq 1$. Then $f$ satisfies a monic polynomial of the form

$$f^n + \alpha_1(x)f^{n-1} + \cdots + \alpha_{n-1}(x)f + \alpha_n(x) = 0,$$

where $\alpha_1, \ldots, \alpha_n \in R$. Substituting $f = p(x)/q(x)$ for $f$ and multiplying both sides by $q^n(x)$, we obtain

$$p(x)^n + \alpha_1(x)q(x)f^{n-1} + \cdots + \alpha_{n-1}(x)q(x)^{n-1}f + \alpha_n(x)q(x)^n = 0.$$

This shows that $q(x)$ divides $p(x)$. Since we are assuming that $q(x)$ and $p(x)$ have no common factors of degree $\geq 1$, this implies that $\deg(q) = 0$, i.e., $f = p(x)/q(x)$ lies in $R$, as claimed.