Solutions to Homework 1.

All rings are commutative with identity!

(1) [4pts] Let R be a finite ring. Show that $R^* = \mathrm{NZD}(R)$.

Proof. Let $a \in \mathrm{NZD}(R)$ and $t_a : R \longrightarrow R$ the map defined by $t_a(r) = ar$ for all $r \in R$. Since a is a nonzero divisor on R, t_a is injective. An injective map from a finite set into itself is surjective. Thus there is an element $b \in R$ with $ab = 1$.

(2) [8pts] Suppose that R is a subring of a ring S and that R is a direct summand of S as an R-module (i.e. $S = R \oplus N$ as an R-module).
(a) Prove that each ideal is the contraction of an ideal of S.
(b) Conclude that R is Noetherian (Artinian) if S is Noetherian (Artinian).

Proof. Suppose that $S = R \oplus N$ as an R-module.

(a) Let $I \subseteq R$ be an ideal. Then $IS = IR \oplus IN$ and $IS \cap R = IR \cap R = I$ since $N \cap R = 0$.

(b) Let $\mathfrak{M} = \{I_\lambda \mid \lambda \in \Lambda\}$ be a set of ideals of R. Then $\mathfrak{M}_S = \{I_\lambda S \mid \lambda \in \Lambda\}$ is a set of ideals in S. If S is Noetherian (Artinian) then $\mathfrak{M}_S$ has a maximal (minimal) element. Since every ideal I_λ is the contraction of $I_\lambda S$, the set $\mathfrak{M}$ has a maximal (minimal) element.

(3) [16pts] Let R be a ring.
(a) Suppose that $I \subsetneq R$ is an ideal which is not principal, but every ideal which properly contains I is principal. Show that I is a prime ideal.
(b) If every prime ideal of R is principal then every ideal of R is principal.

Proof. Assume that $a, b \in R$ with $ab \in I$ and $a \notin I$, $b \notin I$. By assumption:

$$I : (a) = (b_1) \quad \text{with} \quad I + (b) \subseteq (b_1)$$
$$I : (b_1) = (a_1) \quad \text{with} \quad I + (a) \subseteq (a_1)$$

In particular, $a_1 b_1 \in I$. Continue:

$$I : (a_1) = (b_2) \quad \text{with} \quad I + (b_1) \subseteq (b_2)$$
$$I : (b_2) = (a_2) \quad \text{with} \quad I + (a_1) \subseteq (a_2)$$

This yields increasing sequences of ideals in R:

$$I \subseteq (a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$
$$I \subseteq (b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \dots$$

Their unions are principal ideals:

$$(a_0) = \bigcup_{i \in \mathbb{N}} (a_i)$$
$$(b_0) = \bigcup_{i \in \mathbb{N}} (b_i)$$

with $a_0b_0 \in I$, $I : (a_0) = (b_0)$, and $I : (b_0) = (a_0)$. We claim that $I = (a_0b_0)$. If $x \in I$, then $x \in (a_0)$ and $x = a_0 s$ for some $s \in R$. Then $s \in I : (a_0) = (b_0)$ and $s = b_0 t$ for some $t \in R$. Thus $x = a_0 b_0 t$ and $x \in (a_0b_0)$. Contradiction.

(b) Let

$$\mathfrak{M} = \{I \subseteq R \,|\, I \text{ a non-principal ideal}\}$$

be the set of non-principal ideals of R. $\mathfrak{M}$ is partially ordered by inclusion. If $\mathfrak{M}$ is not empty then $\mathfrak{M}$ is inductively ordered. If $\mathfrak{K} = \{I_\lambda\}_{\lambda\in\Lambda}$ is a chain in $\mathfrak{M}$, then $J = \cup_{\lambda\in\Lambda} I_\lambda$ is not a principal ideal in R, since otherwise $J = (a) = I_\lambda$ for some $\lambda \in \Lambda$. Thus $J \in \mathfrak{M}$ and by Zorn's Lemma, $\mathfrak{M}$ has a maximal element I. By part (a), the ideal I is prime and thus principal by assumption, contradiction.

(4) [8pts] Let R be a ring and $S \subseteq R$ a nonempty subset. Show that the following are equivalent:
(a) $R - S$ is the union of prime ideals.
(b) $1 \in S$ and $(ab \in S \Leftrightarrow a \in S \text{ and } b \in S)$.

Proof. (a) $\Rightarrow$ (b) Suppose that Γ is a set of prime ideals of R and that

$$R - S = \bigcup_{P\in\Gamma} P.$$

Then $1 \in S$ and if $ab \in S$ then $ab \notin P$ for all $P \in \Gamma$. Thus $a \notin \cup P$ and $b \notin \cup P$. Therefore $a \in S$ and $b \in S$.

(b) $\Rightarrow$ (a) If $a, b \in S$ then $ab \in S$ and S is multiplicatively closed. If $0 \in S$ then $S = R$. The empty set $R - S$ is the union of an empty set of prime ideals. We may suppose that $0 \notin S$. Theorem (1.12) applied to S and the ideal $I = (0)$ yields that there is a prime ideal $P \subseteq R$ with $P \cap S = \emptyset$. Let Γ be the set of prime ideals Q with $Q \cap S = \emptyset$. Then

$$R - S = \bigcup_{Q\in\Gamma} Q.$$

Obviously, $\cup Q \subseteq R - S$. In order to show the other inclusion, let $a \in R - S$. By assumption (b): $(a) \cap S = \emptyset$ and by Theorem (1.12) there is a prime ideal $P \subseteq R$ with $a \in P$ and $P \cap S = \emptyset$.

(5) [10pts] Let R be an integral domain, $P = \{p_\lambda\}_{\lambda\in\Lambda}$ the set of prime elements of R, and S the multiplicative set generated by P and R^*.
(a) Show that S is saturated.
(b) Show that the following are equivalent:

(i) R is a UFD (factorial).
(ii) $S^{-1}R$ is the quotient field of R.
(iii) Each proper prime ideal of R contains some p_λ.

Proof. (a) Let $a, b \in R$ with $ab \in S$. Then

$$ab = \epsilon p_1 \dots p_r$$

where $\epsilon \in R^*$ and p_i prime elements. Since $p_1, \dots, p_r$ are prime elements, we may assume by renumbering and counting multiplicities correctly that $a = \alpha p_1 \dots p_s$ and $b = \beta p_{s+1} \dots p_r$ where $\alpha, \beta \in R$. Then $\alpha\beta = \epsilon$ and $a, b \in S$.
(b) (i) $\Rightarrow$ (ii) clear

(ii) $\Leftrightarrow$ (iii) Use that the prime ideals Q of $S^{-1}R$ are in $1-1$ correspondence to the prime ideals P of R which satisfy $P \cap S = \emptyset$.
(ii) $\Rightarrow$ (i) Let $x \in R - (R^* \cup \{0\})$. Then there is a $\gamma \in S^{-1}R$ with $(x/1)\gamma = 1/1$. Write $\gamma = a/b$ with $a \in R$ and $b \in S$. Then $xa = b \in S$. By (a) the multiplicative set S is saturated, hence $x \in S$ and x is product of prime elements in R. R is a UFD.

(6) [12pts] Assumptions as in problem (5). Suppose in addition that every nonzero nonunit of R is a finite product of irreducible elements of R. Show that if $S^{-1}R$ is a UFD, then R is a UFD.

Proof. Suppose that $\{p_\lambda\}_{\lambda\in\Lambda}$ is a set of prime elements of R and that S is the multiplicative set generated by $\{p_\lambda\}_{\lambda\in\Lambda}$ and R^*. By the same proof as in (5)(a) the multiplicative set S is saturated. Assume that $S^{-1}R$ is a UFD and that every element $x \in R - (R^* \cup \{0\})$ is a finite product of irreducible elements. In order to show that R is a UFD it suffices to show that every irreducible element of R is a prime element of R. Let $x \in R$ be irreducible.
(a) $x/1 \in S^{-1}R$ is a unit or an irreducible element of R.

If $x/1$ is not a unit, suppose that $x/1 = (a/s)(b/t)$ in $S^{-1}R$ where $a, b \in R$ and $s, t \in S$. Then $xst = ab$ in R. By assumption $s = \alpha p_1 \dots p_n$ and $t = \beta q_1 \dots q_m$ where $\alpha, \beta \in R^*$ and $p_i, q_j \in \{p_\lambda\}_{\lambda\in\Lambda}$. Then for all $1 \le i \le n$, $p_i \,|\, a$ or $p_i \,|\, b$ and for all $1 \le j \le m$, $q_j \,|\, a$ or $q_j \,|\, b$. Thus we can cancel s and t and write $x = a_1 b_1$ where $a_1 \,|\, a$ and $b_1 \,|\, b$. Since x is irreducible in R, a_1 or b_1 is a unit in R. Hence a/s or b/t is a unit in $S^{-1}R$ and $x/1$ is irreducible in $S^{-1}R$.
(b) This shows that if x is irreducible in R then $x/1$ is a unit or a prime element in $S^{-1}R$. If $x/1$ is a unit, then $(x) \cap S \neq \emptyset$ and $x \in S$, since S is saturated. In this case x is a prime element of R. Suppose that $x/1$ is a prime element of R and let $a, b, c \in R$ with $ab = xc$. We have to show that $x \,|\, a$ or $x \,|\, b$. Since $x/1$ is prime in $S^{-1}R$, $(x/1) \,|\, (a/1)$ or $(x/1) \,|\, (b/1)$. Suppose that $(x/1) \,|\, (a/1)$. Then $(*)$ $a/1 = (x/1)(d/e)$ where $d \in R$ and $s \in S$. In particular, $e = \epsilon p_1 \dots p_r$ where $\epsilon \in R^*$ and $p_i \in R$ prime elements. Since e is a product of prime elements we can cancel those with $p_i \,|\, d$ and may assume that $(d, e) = 1$. $(*)$ yields that $ae = xd$ in R. Hence for all $1 \le i \le r$, $p_i \,|\, x$, since $p_i \in R$ prime and $p_i \not| d$. By assumption $x \in R$ is irreducible, hence $x = \alpha p_i$ with $\alpha \in R^*$. But then $x \in S$ and $x/1$ a unit in $S^{-1}R$, a contradiction. This shows that $e = \epsilon \in R^*$ and $x \,|\, a$.

(7) [8pts] Let M be an R-module and $I \subseteq R$ and ideal. Suppose that $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subseteq R$ with $I \subseteq \mathfrak{m}$. Show that $M = IM$.

Proof. Consider the R-module $\bar{M} = M/IM$ and let $\mathfrak{m} \subseteq R$ be a maximal ideal of R. If $I \not\subseteq \mathfrak{m}$ then $I_{\mathfrak{m}} = R_{\mathfrak{m}}$ and $\bar{M}_{\mathfrak{m}} = 0$. If $I \subseteq \mathfrak{m}$ then by assumption $M_{\mathfrak{m}} = 0$ and $\bar{M}_{\mathfrak{m}} = 0$. By the local-global principle $\bar{M} = 0$.

(8) [8pts] Suppose that R is an integral domain. An R-module M is called *torsion free* if for all $a \in R - (0)$ and all $m \in M - (0)$ it holds that $am \neq 0$. Show that M is a torsion free R-module if and only if $M_{\mathfrak{m}}$ is a torsion free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m} \subseteq R$.

Proof. Suppose that $M_{\mathfrak{m}}$ is torsion free for all maximal ideals $\mathfrak{m} \subseteq R$. Let $n \in M$ and $a \in R - (0)$ with $an = 0$. If $n \neq 0$ the annihilator $\operatorname{ann}(n)$ is a proper ideal of R and there is a maximal ideal $\mathfrak{m}$ of R with $\operatorname{ann}(n) \subseteq \mathfrak{m}$. This implies that $n/1 \neq 0$ in

$M_{\mathfrak{m}}$. Since R is an integral domain the canonical map $R \longrightarrow R_{\mathfrak{m}}$ is injective. Let $t \in \operatorname{ann}(n) - (0)$, then $t/1 \neq 0$ in $R_{\mathfrak{m}}$ and $(t/1)(n/1) = 0$ in $M_{\mathfrak{m}}$, a contradiction.

The converse also holds true: Suppose that M is torsion free. Let $\mathfrak{m} \subseteq R$ be a maximal ideal of R. Suppose that $r, t \in R - \mathfrak{m}$, $s \in R$ and $n \in M$ with $(s/t)(n/r) = 0$ in $M_{\mathfrak{m}}$. Then there is an element $u \in R - \mathfrak{m}$ so that $(us)n = 0$ in M. Since M is torsion free either $n = 0$ or $us = 0$. Thus $n/r = 0$ or $s/t = 0$.

(9) [16pts] Let R be a ring and $f = \sum_{i=0}^n a_i x^i \in R[x]$ be an element in the polynomial ring over R. Show:
(a) f is invertible in $R[x]$ if and only if $a_0 \in R^*$ and for all $i \geq 1$: a_i is nilpotent.
(b) f is a zerodivisor in $R[x]$ if and only if there is an element $b \in R - (0)$ so that $bf = 0$.

Proof. (a) $\Leftarrow$: Let $f = \sum_{i=0}^n a_i x^i \in R[x]$ with $a_0 \in R^*$ and a_i nilpotent for all $1 \leq i \leq n$. Then there is an $N \in \mathbb{N}$ so that

$$(\sum_{i=1}^n a_i x^i)^N = 0.$$

With $g = (1/a_0) \sum_{i=1}^n a_i x^i$ we have that

$$(1+g)(1 - g + g^2 - \ldots \pm g^{N-1}) = 0$$

and f is invertible.

$\Rightarrow$ Let $g = \sum_{i=0}^m b_i x^i \in R[x]$ with $fg = 1$. Then $a_0 b_0 = 1$ and $a_0 \in R^*$. The case where $n = 0$ or $m = 0$ is trivial. Assume $n, m \geq 1$.

Claim: For all $0 \leq r \leq m$ it holds that $a_n^{r+1} b_{m-r} = 0$.

The proof of the claim is by induction on r. If $r = 0$ then $a_n b_m = 0$. Suppose that $a_n^{k+1} b_{m-k} = 0$ for all $0 \leq k < r \leq m$. Then

$$a_n^r = a_n^r fg = \sum_{\ell=0}^{n+m} a_n^r (\sum_{i+j=\ell} a_i b_j) x^\ell = 0.$$

Consider the coefficient of x^{n+m-r}:

$$a_n^r (a_n b_{m-r} + a_{n-1} b_{m-r+1} + \ldots + a_{n-r} b_m) = 0.$$

Since $a_n^r b_\ell = 0$ for all $\ell > m - r$ it follows that $a_n^{r+1} b_{m-r} = 0$.

Thus

$$a_n^{m+1} b_0 = 0.$$

Since b_0 is invertible we obtain that $a_n^{m+1} = 0$. Since a_n is nilpotent the element $a_n x^n$ is contained in every maximal ideal of $R[x]$. Thus $h = f - a_n x^n$ is invertible and we can apply the same argument in order to obtain that a_{n-1} is nilpotent, etc.
(b) The backward direction is trivial. In order to prove the forward direction let $f = \sum_{i=0}^n a_i x^i, g = \sum_{i=0}^m b_i x^i \in R[x]$ with $fg = 0$. We may assume that $f \neq 0$ and that g is a polynomial of minimal degree with $fg = 0$. Since $a_n b_m = 0$ the polynomial $a_n g$ is either zero or has a smaller degree than g. Since $f(a_n g_m) = 0$ it follows that $a_n g = 0$.

Claim: $a_i g = 0$ for all $0 \leq i \leq n$.

We show by induction on r that $a_{n-r}g = 0$ for all $0 \leq r \leq n$. We already know that $a_n g = 0$. Suppose the statement is shown for all $0 \leq k < r$. If $a_{n-r}g \neq 0$ then $\deg(g) = \deg(a_{n-r}g)$ since $f(a_{n-r}g) = 0$ and g of minimal degree. This implies that $a_{n-r}b_m$, the leading coefficient of $a_{n-r}g$, is nonzero. The coefficient of x^{n+m-r} of $fg(= 0)$ is:

$$\sum_{i+j=m+n-r} a_i b_j = a_{n-r}b_m + \sum_{i+j=m+n-r; i>n-r} a_i b_j = 0.$$

By induction hypothesis the right hand sum is 0. Thus $a_{n-r}b_m = 0$.

The claim implies that $b_m f = 0$.

(10) [10pts] For any ring R show that $\mathrm{Jrad}(R[x]) = \mathrm{nil}(R[x])$.

Proof. Obviously, $\mathrm{nil}(R[x]) \subseteq \mathrm{Jrad}(R[x])$. Let $f = \sum_{i=0}^{n} a_i x^i \in \mathrm{Jrad}(R[x])$. Then for all $g \in R[x]$:

$$1 - fg \in R[x]^*.$$

Thus, for $g = x$ the polynomial $1 - xf = 1 - \sum_{i=0}^{n} a_i x^{i+1} \in R[x]^*$. By Problem 9: $a_i \in \mathrm{nil}(R)$ for all $0 \leq i \leq n$ and $f \in \mathrm{nil}(R[x])$.