553 Review Rings

39. Let R be a commutative ring with $1 \neq 0$ and let P be a prime ideal of R. Let I and J be ideals of R s.t. $I \cap J \subset P$. Prove that $I \subseteq P$ or $J \subseteq P$.

Proof. Suppose $I \not\subseteq P$. We will show $J \subseteq P$. Let $x \in I$ with $x \notin P$. $\forall\, y \in J$, the product xy is an element of $I \cap J$ (since $x \in I$ so $xy \in I$ and $y \in J$ so $xy \in J$). Thus, $xy \in P$. Since P is a prime ideal, $x \in P$ or $y \in P$. We already know $x \notin P$, so $y \in P$. Thus, $J \subseteq P$.

---

40. Prove a finite integral domain is a field.

Proof 1. Let $x \in R$, $x \neq 0$. Consider the sequence $x, x^2, x^3, x^4, \ldots$ Since R is finite, it follows that $x^i = x^j$ for some $i < j$. Since $x \neq 0$ and R is an integral domain, we have cancellation. Thus, $1 = x^{j-i}$, so $x \cdot x^{j-i-1} = 1$ ($j > i$ so $j - i - 1 \geq 0$). Hence, x is a unit.

Proof 2. Let $\varphi_a : R \to R$ be defined so $\varphi_a(x) = ax$ for $a \neq 0$ an element in R.
$\varphi_a(x+y) - a(x+y) = ax + ay = \varphi_a(x) + \varphi_a(y)$, so φ_a is a group endomorphism on the additive group R.
If $x \in \ker \varphi_a$, then $\varphi_a(x) = ax = 0$. Since R is an integral domain and $a \neq 0$, we get $x = 0$, so φ_a is injective.
Since R is finite and $\varphi_a : R \to R$ is injective, φ_a is surjective.
Thus, $\exists$ be R s.t. $\varphi_a(b) = 1 \in R$. But $\varphi_a(b) = ab$.
Thus, a is a unit.

41. An element x of a ring R is called nilpotent if some power of x is zero. Prove that if x is nilpotent, then $1+x$ is a unit in R.

Proof. Suppose $x \in R$ is nilpotent with $x^n = 0$.
Now, $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$
But $x^n = 0$, so $-1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$.
Since -1 is a unit, $x-1$ is a unit in R. Since $x-1 = -1(1-x)$, it follows that $1-x$ is a unit in R.
We proved this for any nilpotent element x. If we can show that $-x$ is nilpotent, then we have $1-(-x) = 1+x$ is a unit.
Consider $(-x)^n = \underbrace{(-x)(-x)\dots(-x)}_{n \text{ times}}$.
Since $(-x)(-y) = xy \quad \forall x, y \in R$, it follows that
$(-x)^n = (-1)^n (x)^n = (-1)^n \cdot 0 = 0$.
Thus $-x$ is nilpotent, so $1+x$ is a unit.

42. Let R be a non-zero commutative ring with 1. Show that if I is an ideal of R such that $1+a$ is a unit in R for all $a \in I$, then I is contained in every maximal ideal of R.

Proof. By way of contradiction, suppose M is a maximal ideal of R with $I \not\subseteq M$. Then $\exists\, x \in I$ s.t. $x \notin M$.
Consider the ideal $M + (x)$. Since $x \notin M$, $M \subseteq M + (x)$, and $x \in M + (x)$, it follows that $M \subsetneq M + (x)$.
Since M is a maximal ideal, it follows that $M + (x) = (1)$.
Hence, $\exists\, m \in M$ and $r \in R$ s.t. $m + rx = 1$.
Then $m = 1 - rx$. Since $-r \in R$ and $x \in I$, an ideal, it follows that $a := -rx$ is an element of I.
Thus, $m = 1 + a$. But $1 + a$ is a unit in R. Thus, m is a unit in R and $m \in M$. Hence $M = R$, which contradicts that M is a maximal ideal.
Therefore, I is contained in every maximal ideal of R.

43. Let R be an integral domain and F its field of fractions. Let P be a prime ideal in R and $R_P = \{\frac{a}{b} \mid a,b \in R, b \notin P\} \subset F$. Show that R_P has a unique maximal ideal.

Proof. We begin by showing that
$\frac{a}{b}$ is a unit in $R_P \iff \frac{a}{b} \notin (P)R_P$.
($\Rightarrow$): Suppose $\frac{a}{b}$ is a unit in R_P. Then $\exists \frac{c}{d} \in R_P$ s.t. $\frac{ac}{bd} = 1$. i.e., $\exists s \in (R \setminus P)$ s.t. $s(ac - bd) = 0$ in R. Since R is an integral domain and $s \neq 0$ ($0 \in P$, so $0 \notin R \setminus P$), $ac - bd = 0 \Rightarrow ac = bd$. Since $b \notin P$, $d \notin P$ and P is prime, $bd \notin P$. Thus, $ac \notin P$, and in particular, $a \notin P$.
$\therefore \frac{a}{b} \notin (P)R_P$.
($\Leftarrow$): Suppose $\frac{a}{b} \notin (P)R_P$. In particular, $a \notin P$.
Thus, $a \in R \setminus P$. $\therefore \frac{b}{a} \in R_P$. (provided $a \neq 0$).
$\frac{a}{b} \cdot \frac{b}{a} = 1$, so $\frac{a}{b}$ is a unit in R_P.

Since $(P)R_P$ doesn't contain any units, $(P)R_P$ is a proper ideal. Moreover, $\forall \frac{a}{b} \notin (P)R_P$,
$(P)R_P + (\frac{a}{b}) = R_P$, so $(P)R_P$ is a maximal ideal.
Any other ideal either contains a unit or is strictly contained in $(P)R_P$, so it is the unique maximal ideal.

44. Let m and n be relatively prime integers. Show that there is an isomorphism $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.

<u>Proof.</u> Since m and n are relatively prime, in $\mathbb{Z}$, the ideals $(m)+(n)=(1)$, so (m) and (n) are comaximal. Thus, by the Chinese Remainder Theorem, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as rings. Thus, $(\mathbb{Z}_{mn})^{\times} \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}$. Therefore, it suffices to show that $(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} = \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.
Let $(a,b) \in (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}$. Then $\exists\ (c,d) \in \mathbb{Z}_m \times \mathbb{Z}_n$ s.t. $(ac, bd) = (a,b)(c,d) = (1,1)$. Thus, $\exists\ c \in \mathbb{Z}_m$ s.t. $ac=1$ and $\exists\ d \in \mathbb{Z}_n$ s.t. $bd=1$.
So $(a,b) \in \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.
Conversely, Suppose $(a,b) \in \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$. Then $\exists\ c \in \mathbb{Z}_m$ s.t. $ac=1$ and $\exists\ d \in \mathbb{Z}_n$ s.t. $bd=1$.
Then $(a,b)(c,d) = (ac, bd) = (1,1)$, so $(a,b) \in (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}$.
Thus, $(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} = \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.
So $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.

45. Show that if x is non-nilpotent in R, then an ideal P of R which is maximal with respect to (*) not containing x^n for $n = 1, \ldots$ is a prime ideal.

Proof. Suppose $a, b \notin P$. We will show $ab \notin P$.
Consider the ideals $P + (a)$ and $P + (b)$.
$P \subsetneq P + (a)$ and $P \subsetneq P + (b)$ since $a \notin P$, $b \notin P$.
Since P is maximal with respect to not containing x^n for any $n \in \mathbb{N}$, $x^n \in P + (a)$, $x^m \in P + (b)$ for some n and m in $\mathbb{N}$.
Then $x^{n+m} = x^n \cdot x^m \in (P + (a))(P + (b)) \subseteq P + (ab)$.
But $x^{n+m} \notin P$, so it follows that $P \subsetneq P + (ab)$.
Hence, $ab \notin P$. So P is prime.

(*) The actual wording of this problem is awful.
Based on having done questions like this in MA 557, this is what I think it is supposed to say.

46. Let $\mathbb{Q}$ be the field of rational numbers, and $D = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(a) Show that D is a principal ideal domain.

Proof. We will prove something much stronger – that D is a field.
Let $a+b\sqrt{2} \neq 0$. $\frac{1}{a+b\sqrt{2}} \frac{(a-b\sqrt{2})}{(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$.
If $a^2-2b^2 \neq 0$, then we have found an inverse in D for $a+b\sqrt{2}$. If $a^2-2b^2 = 0$, then $a^2 = 2b^2$, so $a = \pm b\sqrt{2}$.
Since a and b are rational numbers, this is impossible.
Thus, D is a field, and hence is trivially a PID.

(b) Show that $\sqrt{3}$ is not an element of D.

Proof. Suppose $\sqrt{3} \in D$. Then $\exists a, b \in \mathbb{Q}$ s.t. $\sqrt{3} = a+b\sqrt{2}$.
Notice $b \neq 0$ or $a = \sqrt{3}$, a contradiction since $a \in \mathbb{Q}$, $\sqrt{3} \notin \mathbb{Q}$.
Then $3 = \sqrt{3}^2 = (a+b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2$.
Then $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ a contradiction, provided $a \neq 0$ and $b \neq 0$.
If $a = 0$, then $\sqrt{3} = b\sqrt{2} \Rightarrow \sqrt{3} \cdot \sqrt{2} = b\sqrt{2} \cdot \sqrt{2}$
i.e., $\sqrt{6} = 2b$, a contradiction since $2b \in \mathbb{Q}$ but $\sqrt{6} \notin \mathbb{Q}$.
Thus, $\sqrt{3} \notin D$.

47. Show that if p is a prime such that $p \equiv 1 \pmod 4$, then x^2+1 is not irreducible in $\mathbb{Z}_p[x]$.

Proof. Since $p \equiv 1 \pmod 4$, $p = a^2+b^2$ for some integers a and b. It follows that $b \not\equiv 0 \pmod p$ or else $a = \sqrt{p}$ or $a^2+b^2 > p$, a contradiction. Thus, b is a unit in $\mathbb{Z}_p$ (since $\mathbb{Z}_p$ is an integral domain).
Claim: ab^{-1} is a root.
$(ab^{-1})^2 + 1 = a^2b^{-2} + 1$.
Since $a^2+b^2 \equiv 0 \pmod p$, it follows that $b^{-2}(a^2+b^2) \equiv 0 \pmod p$, but $b^{-2}(a^2+b^2) = a^2b^{-2} + 1$. Thus, $a^2b^{-2}+1 = 0$ in $\mathbb{Z}_p$, so x^2+1 has a root in $\mathbb{Z}_p[x]$ and hence, is reducible.

---

47. Alternative Proof using Field/Galois Theory.

If $p \equiv 1 \pmod 4$, then $p-1 \equiv 0 \pmod 4$, so 4 divides $p-1$ for all such primes. Consider the field $F_p = \mathbb{Z}_p$. $F_p^\times$ is a cyclic group consisting of $p-1$ elements. Since $4 \mid p-1$, there is an element of order 4 in $F_p^\times$. Call this element a. This element is a primitive 4th root of unity, and hence, $a^2 = -1$. Thus, $a^2+1 = 0$, so $a \in F_p$ is a root of x^2+1, meaning it is reducible in $\mathbb{Z}_p[x]$.

48. Show that if p is a prime such that $p \equiv 3 \pmod 4$, Then x^2+1 is irreducible in $\mathbb{Z}_p[x]$.

Proof. Notice that $p-1 \equiv 2 \pmod 4$. In particular, $4 \nmid p-1$ for all such primes. Now $\mathbb{Z}_p = F_p$, and $F_p^\times$ is a cyclic group of order $p-1$. If $F_p^\times$ had an element of order 4, then by Lagrange's Theorem, $4 \mid p-1$, which is false. If there were an $a \in F_p$ s.t. $a^2 = -1$, then $a^4 = (-1)^2 = 1$. It follows that $a \neq 1$ and $a^3 \neq 1$, so a would be an element of order 4 in $F_p^\times$. Thus, x^2+1 does not have a root in $\mathbb{Z}_p[x]$. Since x^2+1 is of degree 2, it follows that x^2+1 is irreducible in $\mathbb{Z}_p[x]$ for $p \equiv 3 \pmod 4$.

49. Find a simpler description for each of the following rings.

(a) $\frac{\mathbb{Z}[x]}{(x^2-3,\ 2x+4)}$

Let $\varphi: \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{3}]$ be the homomorphism fixing $\mathbb{Z}$ and $\varphi: x \mapsto \sqrt{3}$. φ is surjective ($\varphi(a+bx) = a+b\sqrt{3}$) and $\ker \varphi = (x^2-3)$. Thus, by the First Isomorphism Theorem, $\frac{\mathbb{Z}[x]}{(x^2-3)} \cong \mathbb{Z}[\sqrt{3}]$. Therefore, $\frac{\mathbb{Z}[x]}{(x^2-3,2x+4)} \cong \frac{\mathbb{Z}[\sqrt{3}]}{(2\sqrt{3}+4)}$ by Third Iso. Thm.

$\mathbb{Z}[\sqrt{3}]$ is a PID, so all irreducibles are primes.

$2\sqrt{3}+4 = 2(\sqrt{3}+2) = (1+\sqrt{3})(-1+\sqrt{3})(2+\sqrt{3})$

Let N be the field norm.

$N(1+\sqrt{3}) = 1-3 = -2$, $N(-1+\sqrt{3}) = 1-3 = -2$

Since -2 is prime in $\mathbb{Z}$, $1+\sqrt{3}, -1+\sqrt{3}$ are irreducible, and thus, prime in $\mathbb{Z}[\sqrt{3}]$.

$N(2+\sqrt{3}) = 4-3 = 1$, so $2+\sqrt{3}$ is a unit.

Hence, $(2\sqrt{3}+4) = (1+\sqrt{3})(-1+\sqrt{3})$ (as ideals)

Since $(1+\sqrt{3})$ and $(-1+\sqrt{3})$ are distinct maximal ideals (generated by a nonzero prime element in a PID), they are comaximal.

Thus, by the Chinese Remainder Theorem, $\frac{\mathbb{Z}[\sqrt{3}]}{(1+\sqrt{3})(-1+\sqrt{3})} \cong \frac{\mathbb{Z}[\sqrt{3}]}{(1+\sqrt{3})} \times \frac{\mathbb{Z}[\sqrt{3}]}{(-1+\sqrt{3})}$

Let $f_1: \mathbb{Z} \to \frac{\mathbb{Z}[\sqrt{3}]}{(1+\sqrt{3})}$ and $f_2: \mathbb{Z} \to \frac{\mathbb{Z}[\sqrt{3}]}{(-1+\sqrt{3})}$

$\ker f_1 = 2\mathbb{Z}$, $\ker f_2 = 2\mathbb{Z}$, so by F.I.T., we get

$$\frac{\mathbb{Z}[x]}{(x^2-3,\ 2x+4)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

49(b). $\frac{\mathbb{Z}[i]}{(2+i)}$

Let $\varphi : \mathbb{Z} \to \frac{\mathbb{Z}[i]}{(2+i)}$ be the map $\varphi(x) = x + (2+i)$

$x \in \ker \varphi \Leftrightarrow x + (2+i) = (2+i) \Leftrightarrow x \in (2+i)$.

x is an integer and is a product of $2+i$.

Hence, x is a product of $(2+i)(2-i) = 5$

Thus, $\ker \varphi = 5\mathbb{Z}$.

Therefore, by the First Isomorphism Theorem,

$$\frac{\mathbb{Z}[i]}{(2+i)} \cong \frac{\mathbb{Z}}{5\mathbb{Z}}$$

50. Show that $\mathbb{Z}[\sqrt{-13}]$ is not a Principal Ideal Domain.

Proof. We will show that $\mathbb{Z}[\sqrt{-13}]$ is not a UFD. Since all PIDs are UFDs, this is sufficient.

Consider $(1+\sqrt{-13})(1-\sqrt{-13}) = 14 = 2 \cdot 7$

Let N be the field norm.

$N(2) = 2^2 = 4$. If 2 is reducible, $\exists\ a+b\sqrt{-13}$ with norm 2.

$N(a+b\sqrt{-13}) = a^2 + 13b^2$. If $b \neq 0$, then $a^2+13b^2 > 2$.

Hence, $a^2 = 2$. Since $a \in \mathbb{Z}$, this is a contradiction.

Thus, 2 is irreducible.

We see that $2 \mid (1+\sqrt{-13})(1+\sqrt{-13})$, but $2 \nmid (1+\sqrt{-13})$ and $2 \nmid (1-\sqrt{-13})$. Hence, 2 is <u>not</u> prime.

Since all irreducibles are primes in a UFD, $\mathbb{Z}[\sqrt{-13}]$ is not a UFD.

Thus, $\mathbb{Z}[\sqrt{-13}]$ is not a PID.

51. Let D be a principal ideal domain. Prove that every nonzero prime ideal of D is a maximal ideal.

Proof. Let $P = (p)$ be a prime ideal of D. $(p \neq 0)$.
Let $I = (a)$ be an ideal such that $(p) \subseteq (a) \subseteq D$.
Then $p \in (a)$, so $p = ab$ for some $b \in D$, $(b \neq 0)$.
Then $ab \in (p)$. Since (p) is a prime ideal,
$a \in (p)$ or $b \in (p)$. If $a \in (p)$, then
$(a) \subseteq (p)$, so $(p) = (a)$.
If $b \in (p)$, then $b = cp$ for some $c \in D$.
Thus, $p = ab = acp$. Since PIDs are integral domains, we have cancellation. Thus,
$1 = ac$, so a is a unit, giving $(a) = D$.
Thus, $P = (p)$ is a maximal ideal.

52. Prove or disprove that a nonzero prime ideal P of a principal ideal domain R is a maximal ideal.

Proof. See problem 51.

53. Consider the polynomial $f(x) = x^4+1$

(a) Use the Eisenstein Criterion to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$

Solution. $f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+2$

Since $4, 6, 2 \in (2)$, but $2 \notin (2)^2 = (4)$, $f(x+1)$ is irreducible by Eisenstein.

If $f(x) = p(x)\,q(x)$ is a factorization, then $f(q(x)) = p(q(x))q(q(x))$ is a factorization.

So since $f(x+1)$ is irreducible, so too is $f(x)$.

(b) Prove that $f(x)$ is reducible in $F_p[x]$ for every prime p.

(I don't know how to do this without Galois Theory!)

For $p=2$, $(1)^4+1 = 0$, so it is reducible.

Assume p is odd. Then $p \equiv 1, 3, 5, 7 \pmod 8$. $p^2 \equiv 1 \pmod 8$, in all cases.

Thus, $p^2-1 \equiv 0 \pmod 8$ $\forall$ odd primes p.

Consider the extension F_{p^2}/F_p. The group of units $F_{p^2}^{\times}$ consists of p^2-1 elements, which is divisible by 8.

Thus, $F_{p^2}^{\times}$ contains an element of order 8 (since $F_{p^2}^{\times}$ is a cyclic group and $8 \mid |F_{p^2}^{\times}|$).

Thus, F_{p^2} contains a primitive 8^{th} root of unity, and so contains all primitive 8^{th} roots of unity.

Thus, F_{p^2} contains all roots of $\Phi_8 = x^4+1$.

If x^4+1 were irreducible, it would be the minimal polynomial for ζ_8. Thus, $[F_p(\zeta_8) : F_p] = 4$. But $\zeta_8 \in F_{p^2}$ and $[F_{p^2} : F_p] = 2$. Therefore, x^4+1 is reducible in $F_p[x]$.

54. Assume that $f(x)$ and $g(x)$ are polynomials in $\mathbb{Q}[x]$ and that $f(x)g(x) \in \mathbb{Z}[x]$. Prove that the product of any coefficient of $f(x)$ with any coefficient of $g(x)$ is an integer.

Proof. Let $h(x) = f(x)g(x)$. Since $\mathbb{Z}$ is a UFD and $\mathbb{Q}$ is its field of fractions, Gauss's Lemma gives us that $\exists\, r, s \in \mathbb{Q}$ s.t. $rf(x), sg(x) \in \mathbb{Z}[x]$ and $rf(x)sg(x) = h(x)$.
But then we have $rs\,f(x)g(x) = h(x) = f(x)g(x)$.
By the cancellation law of integral domains, $rs = 1$.
Let a be any coefficient of $f(x)$.
Let b be any coefficient of $g(x)$.
Then by above, $ra \in \mathbb{Z}$ and $sb \in \mathbb{Z}$.
Hence, their product $rasb \in \mathbb{Z}$.
But $rasb = rsab = 1 \cdot ab = ab$.
Thus, the product $ab \in \mathbb{Z}$.

55. Let k be a field, x, y indeterminates. Let $f(x)$ and $g(x)$ be relatively prime polynomials in $k[x]$. Show that in the polynomial ring $k(y)[x]$, $f(x) - y\,g(x)$ is irreducible.

Proof. Since k is a field, $k[y]$ is a UFD. Notice that the field of fractions of $k[y]$ is $k(y)$. By Gauss's Lemma, if we show $f(x) - y\,g(x)$ is irreducible in $k[y][x]$, then we will have shown it irreducible in $k(y)[x]$. But $k[y][x] = k[x][y]$. In this ring, $f(x) - y\,g(x)$ is a degree 1 polynomial in y. This is reducible if and only if the coefficients share a common non-unit factor. But the coefficients are $f(x)$ and $g(x)$, which are relatively prime. Hence, $f(x) - y\,g(x)$ is irreducible in $k[x][y]$ and so too in $k(y)[x]$.