KSOM ALGEBRA II 2021 MAY–AUG
NOTES AND EXERCISES: RING THEORY 1

POSETS AND ZORN'S LEMMA

(1) (Some definitions about posets) A partially ordered set, or poset for short, is a set X with a relation $\leqslant$ that is: (a) reflexive: $x \leqslant x$; (b) anti-symmetric: $x \leqslant y$ and $y \leqslant x$ implies $x = y$; and (c) transitive: $x \leqslant y$ and $y \leqslant z$ implies $x \leqslant z$.

A fundamental example of a poset is the power set of a set with inclusion between subsets being the relation.

Two elements x and y of a poset are comparable if either $x \leqslant y$ or $y \leqslant x$; they are incomparable if they are not comparable. A chain, or totally ordered set, of a poset is a subset any two elements of which are comparable. A subset in which no two elements are comparable is an anti-chain.

An element x is said to be an upper bound of a subset of a poset X if $s \leqslant x$ for every s in S. The notion of a lower bound is similarly defined.

(2) A map f from a poset $(X, \leqslant)$ to a poset $(X', \leqslant)$ is order preserving if $f(x) \leqslant f(y)$ whenever $x \leqslant y$.

(a) Define the notion of an isomorphism of posets. (Note that the inverse of a bijective order preserving map need not be order preserving.)

(b) Determine (as groups) the automorphisms of the following posets: (i) the power set of $[n]$; (ii) the set $\mathbb{Z}$ of integers; (iii) the set $\mathbb{N}$ of natural numbers.

(3) (Amusement) What is the maximal size of an anti-chain in the power set of $[n] := \{1, 2, \ldots, n\}$? You should guess the answer yourself (which is not so hard) and try to prove it (which may be harder) before looking at the footnote, which gives a proof from the Book.[1]

---

[1] Note that the set of subsets of $[n]$ of a given cardinality k form an anti-chain. Choosing $k = \lfloor n/2 \rfloor$, we see that there is an anti-chain of cardinality $\binom{n}{\lfloor n/2 \rfloor}$. We claim that no anti-chain can have larger cardinality. Towards a proof of this, we consider, perhaps counter intuitively at first sight, maximal chains in our poset and their properties. Let M denote the set of all maximal chains, and, for x in the poset, M_x the set of maximal chains containing x. The crucial observation linking anti-chains to maximal chains is this: M_x and M_y are disjoint if x and y are incomparable; thus, for an anti-chain A, the sets M_a, $a \in A$, form a family of pairwise disjoint subsets of M. (Only the fact that the elements of M are chains is used here. That they happen to be maximal is not yet relevant but will soon be.)

Let us now consider the sizes of M and M_x:

(a) Every maximal chain has $n + 1$ elements, and there are $n!$ maximal chains (thus $|M| = n!$).

(b) If x has cardinality k, then M_x has cardinality $k!(n-k)!$. Thus, the minimal possible cardinality of M_x is $m := \lfloor n/2 \rfloor! (n - \lfloor n/2 \rfloor)!$.

We can now finish the proof. Let A be an anti-chain. Given that M_a, $a \in A$, are pairwise disjoint, we have $\sum_{a \in A} |M_a| \leqslant |M| = n!$. On the other hand, since $m \leqslant |M_a|$ for all a, we have $|A| m \leqslant \sum_{a \in A} |M_a|$. Putting the two inequalities together, we see that $|A| \leqslant n!/m = \binom{n}{\lfloor n/2 \rfloor}$. □

(4) (Zorn's lemma and applications) The lemma says: *If every chain of a non-empty poset admits an upper bound, then the poset admits maximal elements.* We will accept this at face value and apply it.[2]
   (a) Every vector space has a basis. (Use Zorn's lemma to conclude that there is a maximal linearly independent set. Any such set is a basis.)
   (b) Let S be a subset of a ring A (not necessarily with identity). If there is a left (respectively right, two-sided) ideal of A not meeting S, then A admits left ideals (respectively right, two-sided) that are maximal with respect to not meeting S.
   (c) Let A be a non-zero ring (with identity). Put $S = \{1\}$ and invoke the previous item to conclude that the poset of proper left (respectively right, two-sided) ideals of A admits maximal elements.

(5) Let $A \neq \{0\}$ be an abelian group. We can turn it into a pseudo-ring (that is, a ring without necessarily having a multiplicative identity) by setting $ab = 0$ for all a, b in A. Now consider the abelian group $\mathbb{Q}/\mathbb{Z}$ made into a pseudo-ring as above. Any subgroup is an ideal. Show that $\mathbb{Q}/\mathbb{Z}$ does not admit maximal proper subgroups, and hence that the pseudo-ring $\mathbb{Q}/\mathbb{Z}$ does not admit maximal (proper) ideals. (Let M be a proper subgroup and let q be in $\mathbb{Z}$ such that $1/q \notin M$ (if $p/q \notin M$, then $1/q \notin M$). Show that $\mathbb{Z}/q + M$ does not contain $1/q^2$ (observe that if $1/q^2 = p/q + m$ for m in M, then $(1 + pq)m = (1 - p^2q^2)/q^2 = 1/q^2$ belongs to M, which means $1/q$ belongs to M, a contradiction). Thus $M \subsetneq \mathbb{Z}/q + M \subsetneq \mathbb{Z}/q^2 + M$.)

(6) (Embedding a pseudo-ring as an ideal of a ring) Let A be a pseudo-ring (that is, a ring perhaps without multiplicative identity). We now construct a ring denoted $\mathbb{Z} \ltimes A$ as follows: it is $\mathbb{Z} \oplus A$ as an abelian group with multiplication defined by:

$$(m, a)\ (n, b) := (mn, ab + na + mb)$$

The element $(1, 0)$ is the multiplicatie identity in this ring. The map $a \mapsto (a, 0)$ is a homomorphism of pseudo-rings. It is an injection and its image $\{(0, a) \mid a \in A\}$ is a two-sided ideal in $\mathbb{Z} \ltimes A$.

1. Examples of Rings (always with identity)

The ambience of a ring (with identity), denoted A, is assumed. Ring homomorphisms are assumed to be unital, meaning that the image of the multiplicative identity under a ring homomorphism is the multiplicative identity.

(1) The **zero-ring**: $\{0\}$. In certain assertions about rings, this has to be excluded explicitly, as for instance in: *every non-zero ring admits a two-sided maximal ideal.*

[2] Timothy Gowers: "If you are building a mathematical object in stages and find that (i) you have not finished even after infinitely many stages, and (ii) there seems to be nothing to stop you continuing to build, then Zorn's lemma may well be able to help you."

(2) The **ring $\mathbb{Z}$ of integers**: There is a unique ring homomorphism from $\mathbb{Z}$ to any given ring. Its image lands in the centre (which by definition comprises all the elements of A that commute with every element of A).

(3) **Rings of functions**: Functions, say real valued, on any set form a ring: addition and multiplication are defined pointwise. The commutativity of the multiplication of real numbers implies that this ring is commutative.

We could also look at restricted classes of functions: e.g., the real valued continuous functions on a topological space form a ring.

(4) **Subrings; Invariant Rings**: We insist that a subring contain the multiplicative identity of A (to be considered a subring of A). The centre of a ring (defined in one of the items above) is a subring.

Suppose that a group acts on a ring by automorphisms. Then the elements of the ring that are left invariant by every element of the group form a subring, called the invariant ring. A basic example of such a situation is provided by the symmetric group $\mathfrak{S}_n$ on n letters acting on the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ by permuting the variables.

(5) **Quotient rings**: Given a two-sided ideal I of A, the space A/I of cosets of I inherits a ring structure from that of A. The quotient ring A/I has the following universal property: any ring homomorphism from A whose kernel contains I uniquely factors through the canonical epimorphism $A \to A/I$.

(6) **Polynomial rings**

(7) **Endomorphisms of abelian groups**

(8) **Endomorphisms of vector spaces (matrix rings)**

(9) **Rings of fractions**

(10) **Group rings**: Here the product is convolution. See item (2) in the next section.

(11) **Direct product of rings**

(12) **Inverse Limits of Rings; Completions**

(13) The **opposite** of a ring.

(14) **Commutants**: Let B be a subset of the ring A and let C be the commutant inside of B, that is, the set of all elements of A that commute with all elements of B. Any such commutant is a subring of A (no matter what subset B is). The commutant of the commutant of B is called the double commutant of B.

The double commutant of B contains the subring generated by B but could in general be strictly larger, as for instance in the following example. Let A be the ring $M_n(\mathbb{C})$ of $n \times n$ complex matrices (with respect to the usual addition and multiplication of matrices), and B be the subring of upper triangular matrices. The commutant of B is the subring of scalar matrices and its double commutant is A.

As another example, consider the subring B of $M_n(\mathbb{C})$ consisting of all diagonal matrices. The commutant of B is itself.

PROBLEMS ABOUT (NOT NECESSARILY COMMUTATIVE) RINGS

As before, A denotes a ring (with identity, not necessarily commutative).

(1) Let $x_1, \ldots, x_n$ be elements of A. For S a subset of $[n] := \{1, 2, \ldots, n\}$, put $x_S := \sum_{s\in S} x_s$. Show that

$$\sum_{S\subseteq[n]} (-1)^{|S|} x_S^n = (-1)^n \sum_{\sigma\in\mathfrak{S}_n} x_{\sigma(1)} \cdots x_{\sigma(n)}$$

(Observe that $x_S = \sum_{(i_1,\ldots,i_n)\in S^n} x_{i_1} \cdots x_{i_n}$. Thus, for a fixed $(i_1, \ldots, i_n)$ in $[n]^n$, the term $x_{i_1} \cdots x_{i_n}$ occurs in x_S (with coefficient 1) if and only if S contains the set $I := \{i_1, \ldots, i_n\}$ (with repetitions removed). Finally, we observe that, for a fixed subset I of $[n]$, $\sum_{S\supseteq I}(-1)^{|S|}$ vanishes except for $I = [n]$ in which case it is $(-1)^n$.)

(2) Consider continuous compactly supported real valued functions on the real line. The convolution product, defined by $(fg)(x) := \int_{\mathbb{R}} f(x-t)g(t)dt$, endows this set of functions with the structure of a (commutative) pseudo-ring, that is, a ring without identity. The delta function supported at the identity (with integral one) would morally be the multiplicative identity but this does not quite belong to our set of functions.

(3) Let V be a finite dimensional vector space over a field k. Let $\mathfrak{E}$ be the ring of k-linear endomorphisms of V. (The ring $\mathfrak{E}$ is isomorphic to the ring $M_{\dim V}(k)$ of $\dim V \times \dim V$ matrices with entries over k, although this isomorphism is not canonical, depending as it does on a choice of basis of V.)

(a) For a subspace U of V, put

$$\ell_U := \{f \in \mathfrak{E} \mid \ker F \supseteq U\} \quad \text{and} \quad \rho_U := \{f \in \mathfrak{E} \mid f(V) \subseteq U\}$$

Observe that ℓ_U is a left ideal and ρ_U is a right ideal.

(b) If $U \subseteq U'$ then $\ell_U \supseteq \ell_{U'}$ and $\rho_U \subseteq \rho_{U'}$.

(c) $\ell_U = \mathfrak{E}f$ for any $f \in \mathfrak{E}$ with $\ker f = U$, and $\rho_U = f\mathfrak{E}$ with any $f \in \mathfrak{E}$ with $\operatorname{Im} f = U$.

(d) Every left ideal ℓ is of the form ℓ_U for some subspace U. In fact, we can take U to be $\cap_{f\in\ell} \ker f$. (The goal is to prove that $\ell = \ell_U$. It is evident from the definition of ℓ_U that $\ell \subseteq \ell_U$. For the other inclusion, it suffices to show, by item (3c) above, that there is an f in ℓ with $\ker f = U$. Choose $f \in \ell$ such that $\ker f$ is minimal (with respect to inclusion). We have $\ker f \supseteq U$. We claim that $\ker f = U$. Suppose not. Choose $v \in \ker f \backslash U$ and let $g \in \ell$ such that $gv \neq 0$. Observe that $\operatorname{Im} f \subsetneq V$ (since $\ker f$ is non-trivial) and so there exists $y \in \mathfrak{E}$ such that $y(g(v)) \neq 0$ and $\operatorname{Im} y \cap \operatorname{Im} f = 0$. The endomorphism $f + yg$ belongs to ℓ, and $\ker f + gv \subsetneq \ker f$ (since $v \in \ker f$ but $(f + yg)(v) \neq 0$). This contradicts the minimality of $\ker f$. $\square$)

(e) Every right ideal is of the form ρ_U for some subspace U.

(f) If ℓ is a non-zero left ideal, given any element v of V, there exists f in ℓ such that $v \in \mathrm{Im}\, f$. If ρ is a non-zero right ideal, given any element v of V, there exists f in ρ such that $f(v) \neq 0$.

(g) Suppose that I is a non-zero two-sided ideal. Since I is a non-zero right ideal, it follows, from the previous item, that $\cap_{f \in I} \ker f = 0$. Since I is a left ideal, we have $I = \ell_0 = \mathfrak{E}$ (by item (3d)). This proves that $\mathfrak{E}$ is a simple ring in case $V \neq 0$ (that is, it admits exactly two two-sided ideals, namely 0 and itself).

(4) Let V and $\mathfrak{E}$ be as in item (3) above, except that we now assume V to be infinite dimensional. Then $\mathfrak{E}$ is not simple: the endomorphisms of finite rank form a two-sided ideal (which is neither 0 nor the whole of $\mathfrak{E}$).

Commutative rings (always with identity)

The ambience of a commutative ring (with identity), denoted A, is assumed. Ring homomorphisms are assumed to be unital, meaning that the image of the multiplicative identity under a ring homomorphism is the multiplicative identity.

(1) Let I be an ideal and A/I the quotient ring. Every ideal of A/I is of the form J/I for a unique ideal J of A that contains I. This sets up an order preserving bijection between the poset of ideals of A/I and that of the ideals of A that contain I.

(2) A subset S is a multiplicative set if it is closed under multiplication (that is, $xy \in S$ for $x \in S$ and $y \in S$) and contains 1.

(a) The product $ST := \{st \,|\, s \in S, t \in T\}$ of multiplicative sets S and T is a multiplicative set.

(b) If S is a multiplicative set and $\mathfrak{a}$ an ideal, then the set $S + \mathfrak{a} := \{s + a \,|\, s \in S, a \in \mathfrak{a}\}$ is a multiplicative set.

(3) An element x is a unit if there exists an element y such that $xy = 1$; it is a zero-divisor if there exists an element y such that $0 \neq y$ and $xy = 0$; it is a non-zero-divisor, or nzd, if it is not a zero divisor. Units are nzds.

(4) The ring A is a field if it is non-zero and every non-zero element of it is a unit. The following conditions on A are equivalent: (a) A is a field; (b) A has exactly two ideals (the zero ideal and the whole ring); (c) Every homomorphism from A to a non-zero ring is an injection.

(5) An ideal that is maximal (under inclusion) among proper ideals is said to be maximal. If I is a proper ideal, there do exist maximal ideals that contain I (by Zorn). In particular, the ring admits maximal ideals if it is non-zero.

(6) The following are equivalent for an ideal $\mathfrak{m}$: (a) it is maximal; (b) $A/\mathfrak{m}$ is a field; (c) There is an onto ring homomorphism from A to a field with $\mathfrak{m}$ as kernel. Thus, maximal ideals arise as kernels of epimorphisms from A to fields.

(7) The ring A is an integral domain if it is non-zero and has no non-zero zero divisors.
   (a) Any subring of an integral domain is an integral domain.
   (b) Fields are integral domains.
   (c) A finite integral domain is a field.
   (d) Let k be a field and a subring of A. Suppose that the dimension of A as a vector space over k is finite and that A is an integral domain. Then A is a field. (Hint: For $0 \neq a$ in A, consider the powers of a. There must be a non-trivial linear dependence relation over k among them.)

(8) A proper ideal $\mathfrak{p}$ is prime if $xy \in \mathfrak{p}$ implies either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ (for x, y elements of A). The following are equivalent for an ideal $\mathfrak{p}$ of A: (a) $\mathfrak{p}$ is prime; (b) $A \backslash \mathfrak{p}$ is a multiplicative set; (c) the quotient ring $A/\mathfrak{p}$ is an integral domain.

(9) Maximal ideals are prime (since fields are in particular integral domains). In fact, ideals that are maximal with respect to not meeting a fixed multiplicative set are prime.

(10) Every non-zero ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for a positive integer n, the integer n being identified as the smallest positive integer contained in the ideal. The ideal $n\mathbb{Z}$ (where $n \geqslant 0$) is prime if and only if n is either zero or a prime; it is maximal if $n \neq 0$ and a prime.

(11) ("Modular law") $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{b} + (\mathfrak{a} \cap \mathfrak{c})$ for ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ such that $\mathfrak{a} \supseteq \mathfrak{b}$.

(12) Let $\mathfrak{a}$ be an ideal and x an element. The corresponding colon ideal is defined as follows: $(\mathfrak{a} : x) := \{y \in A \mid yx \in \mathfrak{a}\}$.
   (a) $(\mathfrak{a} : x) \supseteq \mathfrak{a}$; $(\mathfrak{a} : x) = A$ iff $x \in \mathfrak{a}$; $(\mathfrak{a} + \mathfrak{b} : x) \supseteq (\mathfrak{a} : x) + (\mathfrak{b} : x)$
   (b) $(\mathfrak{a} \cap \mathfrak{b} : x) = (\mathfrak{a} : x) \cap (\mathfrak{b} : x)$; $((\mathfrak{a} : x) : y) = (\mathfrak{a} : xy)$.
   (c) Suppose that $(\mathfrak{a} : x)$ is maximal among proper ideals of that form. Then $(\mathfrak{a} : x)$ is prime.

(13) In each of the following cases, find k such that $k\mathbb{Z}$ equals (a) $m\mathbb{Z} + n\mathbb{Z}$; (b) $m\mathbb{Z} \cap n\mathbb{Z}$; (c) $(m\mathbb{Z} : n)$; (d) $\mathfrak{r}(m\mathbb{Z})$.

(14) An element x is nilpotent if $x^n = 0$ for some integer $n \geqslant 1$.
   (a) All the nilpotent elements together form an ideal, called the nilradical.
   (b) If x is nilpotent, then $1 - x$ is a unit. (Hint: $(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n$.) More generally, $U + \mathfrak{n} \subseteq U$, where U is the multiplicative set of units and $\mathfrak{n}$ the nilradical.
   (c) The nilradical is the intersection of all the prime ideals.

(15) Let $\mathfrak{a}$ be an ideal. The radical of $\mathfrak{a}$, denoted $\mathfrak{r}(\mathfrak{a})$, is by definition the set of all elements x of the ring such that x^n belongs to $\mathfrak{a}$ for some integer $n \geqslant 1$ (depending upon x). We say that the ideal $\mathfrak{a}$ is radical if it equals $\mathfrak{r}(\mathfrak{a})$.
   (a) $\mathfrak{r}(\mathfrak{a})$ is an ideal.
   (b) $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{r}(\mathfrak{a}) \subseteq \mathfrak{r}(\mathfrak{b})$; $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$; $\mathfrak{r}(\mathfrak{a}) = A \Leftrightarrow \mathfrak{a} = A$.
   (c) $\mathfrak{r}(\mathfrak{a})$ is the intersection of all prime ideals containing $\mathfrak{a}$.

(16) The Jacobson radical of A is defined to be the intersection of the all the maximal ideals of A. An element x of A belongs to the Jacobson radical if and only if $1 - xy$ is a unit for any element y of A.

(17) Let $A[x]$ be the polynomial ring in the indeterminate x with coefficients in A, and let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x)$ be elements of $A[x]$.
  (a) $f(x)$ is nilpotent $\Leftrightarrow$ the a_i are nilpotent for all $0 \leqslant i \leqslant n$.
  (b) $f(x)$ is a unit $\Leftrightarrow$ a_0 is a unit (in A) and the a_i are nilpotent for $i \geqslant 1$.
  (c) $f(x)$ is a zero divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af(x) = 0$.
  (d) (Gauss's Lemma) $f(x)g(x)$ is primitive $\Leftrightarrow$ $f(x)$ and $g(x)$ are both primitive. (A polynomial is primitive if its coefficients generate the unit ideal of A.)

(18) The nilradical and Jacobson radical of $A[x]$ are equal.

(19) A multiplicative set S is saturated if $xy \in S$ implies $x \in S$ and $y \in S$ (for elements x, y of the ring A).
  (a) The units form a saturated multiplicative set. So do the nzds.
  (b) A multiplicative set is saturated if it is the complement of a union of ideals.
  (c) The complement of a saturated multiplicative set is a union of ideals. In fact, it is a union of prime ideals.
  (d) The complement of the set of units is the union of all maximal ideals.
  (e) The set of nzds equals $\cup_{x \neq 0} \mathfrak{r}(\mathrm{Ann}(x))$, where $\mathrm{Ann}(x) := \{y \in A \mid yx = 0\}$ is the annihilator of x.

(20) Let S be a multiplicative set. The saturation $\overline{S}$ of S is the smallest saturated multiplicative set containing S. It exists:
  (a) $\overline{S}$ is the intersection of all saturated multiplicative sets containing S.
  (b) $\overline{S} = \{x \mid \exists\, y \in A$ such that $xy \in S\}$
  (c) $A \backslash S$ is the union of all ideals (respectively, prime ideals) not meeting S.
  (d) $\overline{S} = A \Leftrightarrow 0 \in \overline{S} \Leftrightarrow 0 \in S$.
  (e) The multiplicative set consisting of the units is the saturation of $\{1\}$.

(21) Let S be a multiplicative set not containing 0. (An important instance of this is when A is non-zero and $S = \{1\}$.) Then there exist multiplicative sets maximal with respect to containing S and not containing 0 (by Zorn). Let T be such a maximal multiplicative set. Then:
  (a) T is saturated.
  (b) The complement of T is a minimal prime ideal.
  (c) Given a prime ideal $\mathfrak{p}$, apply the above with $S = A \backslash \mathfrak{p}$ to conclude that there exists a minimal prime contained inside $\mathfrak{p}$.

(22) Let S be multiplicative set and $\mathfrak{a}$ an ideal.
  (a) $S + \mathfrak{a}$ does not contain zero if and only if S does not meet $\mathfrak{a}$.
  (b) The saturation of $S + \mathfrak{a}$ is the complement of the union of ideals containing $\mathfrak{a}$ and not meeting S.

(23) (Criterion for a prime to be minimal) A prime ideal $\mathfrak{p}$ is minimal if and only if: For every x in $\mathfrak{p}$ there exists y not in $\mathfrak{p}$ such that $x^n y$ is nilpotent.

(24) Let $A = C[0,1]$ be the ring of continuous real valued functions on the compact interval $[0,1]$. For $x \in [0,1]$, let $\mathfrak{m}_x$ denote the ideal of elements of A that vanish at the point x.
   (a) Each $\mathfrak{m}_x$ is maximal.
   (b) The $\mathfrak{m}_x$ are all the maximal ideals.
   (c) None of the $\mathfrak{m}_x$ is a minimal prime.

(25) An ideal $\mathfrak{q}$ is primary if the following condition holds:
   for elements x, y such that $xy \in \mathfrak{q}$, either $x \in \mathfrak{q}$ or $y \in \mathfrak{r}(\mathfrak{q})$.
   (a) An ideal $\mathfrak{q}$ is primary if and only if every nzd in $A/\mathfrak{q}$ is nilpotent.
   (b) What are the primary ideals in the ring $\mathbb{Z}$?
   (c) The radical of a primary ideal is prime. If $\mathfrak{q}$ is primary with $\mathfrak{r}(\mathfrak{q}) = \mathfrak{p}$, we say that $\mathfrak{q}$ is $\mathfrak{p}$-primary.
   (d) The intersection of two $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary. In general, however, the intersection of primary ideals is not primary (example?).
   (e) Any ideal whose radical is a maximal ideal is primary.

(26) Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal if $\mathfrak{a} + \mathfrak{b} = A$.
   (a) $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$ if $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal.
   (b) If $\mathfrak{a}$, $\mathfrak{b}$ are comaximal and $\mathfrak{a}$, $\mathfrak{c}$ are comaximal, then $\mathfrak{a}$, $\mathfrak{bc}$ are comaximal.
   (c) If $\mathfrak{a}$, $\mathfrak{b}$ are comaximal, then so are $\mathfrak{a}^m$, $\mathfrak{b}^n$ for any positive integers m, n.
   (d) If $\mathfrak{r}(\mathfrak{a})$, $\mathfrak{r}(\mathfrak{b})$ are comaximal, then so are $\mathfrak{a}$, $\mathfrak{b}$.
   (e) (Chinese Remainder Theorem) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ be ideals. The natural map
   $$A \to \frac{A}{\mathfrak{a}_1} \times \frac{A}{\mathfrak{a}_2} \times \cdots \times \frac{A}{\mathfrak{a}_k}$$
   is onto if and only if $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ are pairwise comaximal. The kernel in that case is $\mathfrak{a}_1 \cdots \mathfrak{a}_k$. (Observe that the kernel is $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ in any case.)

(27) Let $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals. Suppose that $\mathfrak{a} \subseteq \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_n$.
   (a) Suppose that the containment $\mathfrak{a} \subseteq \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_n$ is irredundant, meaning that it does not hold if any one of the ideals in the union on the right is dropped. Then:
      (i) $n \neq 2$. (Suppose that $n = 2$. Let a_2 be in $\mathfrak{a} \backslash \mathfrak{a}_1$ and a_1 be in $\mathfrak{a} \backslash \mathfrak{a}_2$. Then $a_1 + a_2$ belongs to $\mathfrak{a}$ but not to either of $\mathfrak{a}_1$, $\mathfrak{a}_2$.)
      (ii) None of the ideals $\mathfrak{a}_i$ is prime. (Suppose that one of them, say $\mathfrak{a}_n$, is prime. For $1 \leqslant i \leqslant n$, Let a_i be in $\mathfrak{a} \backslash (\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_{i-1} \cup \mathfrak{a}_{i+1} \cup \cdots \cup \mathfrak{a}_n)$. Such an a_i exists by irredundancy. Consider $a_n + a_1 \cdots a_{n-1}$. This belongs to $\mathfrak{a}$, but not to $\mathfrak{a}_i$ (because a_i but not a_n belongs to $\mathfrak{a}_i$) and not to $\mathfrak{a}_n$ (since $a_1 \cdots a_{n-1}$ does not belong to $\mathfrak{a}_n$ by primality of $\mathfrak{a}_n$, but $\mathfrak{a}_n$ does), which is a contradiction.)
   (b) (Prime Avoidance) Suppose that all but at most two of $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are prime. Then $\mathfrak{a} \subseteq \mathfrak{a}_i$ for some i, $1 \leqslant i \leqslant n$. (We may suppose, by deleting some of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ as necessary, that the containment is irredundant. It follows from the previous item that a contradiction ensues unless $n = 1$.)

(28) The ring A is local if it admits only one maximal ideal. The following are equivalent conditions for A to be local:
   (a) The non-units form an ideal.
   (b) For every non-unit x of the ring, $1 - x$ is a unit.