(1) (For those who know topology). Let $X$ and $Y$ be topological spaces and let $X \times Y$ be the usual product space. Prove that $X \times Y$ with the projections on $X$ and $Y$ is a product of $X$ and $Y$ in the category of topological spaces and continuous functions.

We need to show that we have a final object in the category whose objects are spaces $Z$ together with continuous maps from $Z$ to $X$ and $Y$ (and whose arrows are continuous maps “making everything commute”). Let $f : Z \to X$ and $g : Z \to Y$ be the maps, and note that the only function from $Z$ to $X \times Y$ that can possibly work is $h : z \mapsto (f(z), g(z))$. So all we need to do is show that $h$ is continuous: the basic open sets in $X \times Y$ are of form $U \times V$ where $U$ and $V$ are open in $X$ and $Y$ respectively, and $h^{-1}[U \times V] = f^{-1}[U] \cap g^{-1}[V]$ which is open since $f$ and $g$ are continuous.

Cultural note: it is considerations of this sort which motivate the definition of the product topology in an infinite product of topological spaces $\prod_{i \in I} X_i$. Given a space $Z$ and continuous $h_i : Z \to X_i$, we want the map $h : Z \to \prod_i X_i$ given by $h(z)(i) = h_i(z)$ to be continuous; this is so because basic open sets are of form $\prod_i U_i$ with $U_i = X_i$ outside a finite set $I_0 \subseteq I$, so the inverse image of such a basic open set is $\bigcap_{i \in I_0} h_i^{-1}[U_i]$ which is open since the class of open sets is closed under finite intersections.

(2) A coproduct of $A$ and $B$ consists of an object $C$ and maps $i_A$ from $A$ to $C$, $i_B$ from $B$ to $C$ satisfying the following universal property: for any object $D$ and maps $j_A$ from $A$ to $D$, $j_B$ from $B$ to $D$ there is a unique map $k$ from $C$ to $D$ such that $j_A = k \circ i_A$, $j_B = k \circ i_B$.

(a) Prove that if $R$ is a ring, any pair of $R$-modules has a coproduct. Hint: it is a familiar module.

Given modules $A$ and $B$ let $C$ be the direct sum $A \oplus B$ and let $i_A : a \mapsto (a, 0)$, $i_B : b \mapsto (0, b)$. Given $j_A$ and $j_B$ mapping $A$ and $B$ to some module $D$. If there is a suitable HM $k$ then it must be given by $k(a, b) = k(a, 0) + k(0, b) = k(i_A(a)) + k(i_B(b)) = j_A(a) + j_B(b)$.

It is routine to check this is a HM which works.

(b) (Harder) Do coproducts exist in the category of topological spaces and continuous functions? What about the category of groups and homomorphisms?

Groups: yes there is a coproduct. Given $G$ and $H$ form the free group on $G \cup H$ and quotient out by the subgroup generated by $e_G, e_H$, $g_1g_2g_3$ with $g_1g_2g_3 = e$ in $G$, and $h_1h_2h_3$ with $h_1h_2h_3 = e$ in $H$. Now check this works.
Spaces: WLOG $X$ and $Y$ are disjoint. Let $Z = X \cup Y$ and topologise $Z$ by letting $W \subseteq Z$ be open iff $W \cap X$ is open in $X$, $W \cap Y$ is open in $Y$. It is easy to see that this is a topology, that the injections of $X$ and $Y$ into $Z$ are continuous, and that if $f$ and $g$ are continuous maps to $W$ then $f \cup g$ is continuous from $Z$ to $W$.

Note: several people asked why the product is not a coproduct in the category of groups. The big problem is the product amalgamates $G$ and $H$ in such a way that elements of $G \times \{e\}$ commute with elements of $\{e\} \times H$. For example if we take maps $f$ and $g$ from $\mathbb{Z}/2\mathbb{Z}$ to $S_3$ such that $f(1) = (12)$ and $g(1) = (23)$ there is no way to factor through the product.

(3) An $R$-module $P$ is projective if and only if for all $R$-modules $A$ and $B$ and HM $f : P \to B$, surjective $g : A \to B$ there exists a HM $h : P \to A$ such that $f = g \circ h$. Note: there is no uniqueness demand on the map $h$ here.

Prove that free $R$-modules are projective, and that if $R$ is a PID then all fg projective $R$-modules are free. Find an example of a non-free fg projective $R$-module.

Let $P$ be free and let $X$ be a free generating set for $P$. Find a function $h$ such that $g(h(a)) = f(a)$ for every $a \in X$ and use freeness to extend $h$ to a HM from $P$ to $A$. By linearity $f = g \circ h$.

Now let $P$ be a fg projective $R$-module for a PID $R$. Let $a_1, \ldots, a_n$ be a generating set for $P$. Let $F$ be a free module of rank $n$ and let $g$ from $F$ to $P$ be some surjective HM. Apply the defn of projective with $B = P$, $A = F$, $f = id_P$ and get a map $h : P \to F$ such that $id = g \circ h$. This implies that $h$ sets up an IM between $P$ and $h[P]$, but by the structure theory for fg modules over a PID we know that $h[P]$ must be free. Hence $P$ is free.

**STILL OWE AN EXAMPLE OF A PROJECTIVE NON FREE MODULE.**

(4) Let $Z$ be a non-empty set. A pregeometry on $Z$ is a map $cl$ from subsets of $Z$ to subsets of $Z$ satisfying the axioms

(a) $X \subseteq cl(X)$.
(b) $X \subseteq cl(Y) \implies cl(X) \subseteq cl(Y)$.
(c) If $a \in cl(X)$ then $a \in cl(Y)$ for a finite $Y \subseteq X$.
(d) If $a \in cl(X \cup \{b\}) \setminus cl(X)$ then $b \in cl(X \cup \{a\})$.

Check that if $Z$ is a $k$-vector space and $cl(X)$ is the least subspace containing $X$, then $cl$ satisfies these axioms.

Boring.

Let $cl$ be an arbitrary pregeometry on an arbitrary set $Z$.

(a) Show that $X \subseteq Y$ implies $cl(X) \subseteq cl(Y)$, and $cl(cl(X)) = cl(X)$.

If $X \subseteq Y$ then we have $X \subseteq Y \subseteq cl(Y)$ by Axiom 1, and so $cl(X) \subseteq cl(Y)$ by Axiom 2. Now $cl(X) \subseteq cl(cl(X))$ by Axiom 1, and applying Axiom 2 to the trivial inclusion $cl(X) \subseteq cl(X)$ we get $cl(cl(X)) \subseteq cl(cl(X))$.

(b) $X$ is called independent if $x \notin cl(X \setminus \{x\})$ for all $x \in X$. Show that every independent set is contained in a maximal independent set.

Zorn’s lemma. The key point is that a union of a chain of independent sets is independent, this is true by Axiom 3.
(c) Show that the following are equivalent for an independent set $X$.
   (i) $X$ is a maximal independent set.
   (ii) $cl(X) = Z$.

   If either property holds the independent set $X$ is called a basis.

   Suppose $X$ is maximal independent and $z \in Z$. If $z \in X$ we are done, otherwise $X \cup \{z\}$ is not maximal so there is $y \in X \cup \{z\}$ with $y \in cl(X \cup \{z\}\setminus \{y\})$. If $y = z$ then $z \in cl(X)$ and we are done, so assume $y \in X$. By independence $y \notin cl(X\setminus \{y\})$, so applying Axiom 4 $z \in cl(X)$.

   Conversely let $X$ be independent and $cl(X) = Z$. If $z \notin X$ then $X \cup \{z\}$ is not independent because $z \in cl(X \cup \{z\}\setminus \{z\})$.

(d) Prove that any set $X$ with $cl(X) = Z$ contains a basis.

   Use Zorn to find $W \subseteq X$ a maximal independent subset of $X$. We claim that $X \subseteq cl(W)$. If not let $x \in X$ with $x \notin cl(W)$ and consider $W \cup \{x\}$. It is easy to see (similar arguments to last part) that $W \cup \{x\}$ is independent, contradicting maximal choice of $W$. Now $X \subseteq cl(W)$ implies that $Z = cl(X) \subseteq cl(W)$, so $cl(W) = Z$ and $W$ is a basis.

(e) Prove that if $A$ is a basis and $b$ is not in $cl(\emptyset)$ then there is $a \in A$ such that $A \setminus \{a\} \cup \{b\}$ is a basis. Hint: look at a finite subset $A'$ of minimal size with $b \in cl(A')$.

   If $b \in A$ we may let $a = b$ so we assume $b \notin A$. Taking the hint let $A'$ be minimal with $b \in cl(A')$. Since $b \notin cl(\emptyset)$, we may choose $a \in A'$. We will show that $A \setminus \{a\} \cup \{b\}$ is a basis. The key point is that $b \notin cl(A' \setminus \{a\})$, and so $a \in cl(A' \setminus \{a\} \cup \{b\})$. It follows that $a \in cl(A \setminus \{a\} \cup \{b\})$, so that $A \subseteq cl(A \setminus \{a\} \cup \{b\})$ and hence $Z = cl(A) \subseteq cl(A \setminus \{a\} \cup \{b\})$.

   We finish by showing $A \setminus \{a\} \cup \{b\}$ is independent. If $b$ is in $cl(A \setminus \{a\})$ then $A' \setminus \{a\} \cup \{b\}$ is contained in $cl(A \setminus \{a\})$, implying that $a \in cl(A \setminus \{a\})$ and contradicting the independence of $A$. If $a' \in A \setminus \{a\}$ and $a' \in cl(A \setminus \{a,a'\} \cup \{b\})$, then as usual $a' \notin cl(A \setminus \{a,a'\})$ and so $b \in cl(A \setminus \{a\})$.

(f) Show that if there exists a finite basis, then all other bases have the same size.

   Note that no element in $cl(\emptyset)$ appears in any basis. Given a finite basis $A$ and a basis $B$, use the method of the last lemma to successively replace elements of $A$ by elements of $B$. Argue that once elements of $B$ go in they are never taken out again. Argue that no elements of $A$ can remain, so that $A$ has the same size of $B$.

   Hint: if you get stuck, look at the proof for vector spaces. If you are ambitious and know a bit of set theory, prove that in general any two bases are of the same (possibly infinite) size.

   If $A$ is infinite, wellorder it and repeat the same proof.

(5) Let $k$ be a subfield of $l$. Show that if $A$ is a subset of $l$ then $k(A)$ is the set of elements of the form $f(\vec{a})/g(\vec{a})$ where $f, g \in k[x_1, \ldots, x_n]$ and $\vec{a} \in A^n$ for some $n$, and $g(\vec{a}) \neq 0$.

   Let $B$ be the set of these elements. It is easy to see that $B$ contains $A$ and $k$ and is closed under the field operations, so $k(A) \subseteq B$. Conversely
any element of $B$ can be built from elements of $k$ and $A$ by finitely many applications of the field operations so $B \subseteq k(A)$.

Let $acl(A)$ be the set of elements of $l$ which are algebraic over $k(A)$. Prove that $acl$ is a pregeometry. In this instance an independent set is called algebraically independent and a basis is called a transcendence basis. The (well defined) cardinality of a transcendence basis is called the transcendence degree of $l$ over $k$. Find the transcendence degree of $k(x)$ over $k$. The first three axioms are easy. Suppose that $b$ is algebraic over $k(A \cup \{a\})$, then we can find $a_1, \ldots, a_n \in A$ and $f_i \in k[x_1, \ldots, x_n, y]$ not all zero such that $\sum_{j=1}^n f_i(a_1, \ldots, a_n, a)b^j = 0$. If $b$ is not algebraic over $k(A)$ then $a$ must appear in some coefficient, and rearranging we get that $a$ is algebraic over $k(A \cup \{b\})$.

Finally we see $\{x\}$ is a transcendence basis so the transcendence degree is one.

(6) Let $P$ be the ideal generated by the polynomial $x^2 - y^3$ in $\mathbb{C}[x, y]$. Prove that $P$ is prime. Hint: use the fact that $\mathbb{C}[x, y]$ is a UFD.

$x^2 - y^3$ is irreducible and it follows easily that $P$ is prime.

Let $R = \mathbb{C}[x, y]/P$ and let $F$ be the field of fractions of $R$. Prove that the map $\varphi : a \mapsto a + P$ is a monomorphism from $\mathbb{C}$ to $F$.

\[ \mathbb{C} \cap P = (0) \]

If $k = im(\varphi)$, what is the transcendence degree of $F$ over $k$?

Let $k = im(\varphi)$, $\bar{x} = x + P$, $\bar{y} = y + P$. $\bar{y}$ is algebraic over $\bar{k}(\bar{x})$ because $\bar{y}^2 = \bar{x}^3$. We claim that $\bar{x}$ is transcendental over $\bar{k}$; the point is that $k[x] \cap P = (0)$. Thus $\{\bar{x}, \bar{y}\}$ is a transcendence basis.

(7) Find the algebraic integers in $\mathbb{Q}(\sqrt{5})$.

By an old homework exercise we need to find those rational $a$ and $b$ such that $2a, a^2 - 5b^2$ are both integers. $a = m/2$ for some integer $m$ and so easily $b = n/2$. We need that $m^2 - n^2$ is a multiple of 4, which happens when $m$ and $n$ have the same parity. A little thought shows that the ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = (1 + \sqrt{5})/2$.

(8) If $\phi : R \rightarrow S$ is a ring HM and $I$ is an ideal of $S$ then the contraction $I^c$ of $I$ is the ideal $\phi^{-1}[I]$. Prove that $\phi$ induces a monomorphism from $R/I^c$ to $S/I$. Prove that if $I$ is prime then $I^c$ is prime, but that in general $I$ maximal does not imply that $I^c$ is maximal.

Consider the composition of the map $\phi$ from $R$ to $S$ and the quotient map from $S$ to $S/I$. The kernel of this composite map is $I^c$, so by the first IM thm we get an induced map from $R/I^c$ to $S/I$ given by $r + I^c \mapsto \phi(r) + I$.

$I$ prime implies $S/I$ is an ID implies $R/I^c$ is an ID (any subring of an ID is an ID) implies $I^c$ prime. Consider the natural inclusion map from $\mathbb{Z}$ and the ideal $(0)$ in $R$ to see that the contraction of a maximal ideal need not be maximal.

(9) Prove that $\mathbb{Z}[i]$ is a Euclidean domain.

Easy, use the square of the absolute value.

Prove that if $z \in \mathbb{Z}[i]$ and $|z|^2$ is prime in $\mathbb{Z}$ then $z$ is prime in $\mathbb{Z}[i]$.

Note that $|w|^2$ is always an integer. If $z = ab$ then $|z|^2 = |a|^2|b|^2$, so one of $|a|$ and $|b|$ must be a unit.
Prove that if $p$ is prime in $\mathbb{Z}$ then either $p$ is prime in $\mathbb{Z}[i]$ or $p = Q\bar{Q}$, where $Q$ and its conjugate $\bar{Q}$ are primes of $\mathbb{Z}[i]$ with $|Q|^2 = |\bar{Q}|^2 = p$.

If $p$ is not prime $p$ must have a factorisation into nonunits of $\mathbb{Z}[i]$ as $QR$. $p^2 = |Q|^2|R|^2$, so $|Q|^2 = |R|^2 = p$. By the last part each of $Q$ and $\bar{R}$ is prime in $\mathbb{Z}[i]$. It follows easily that $Q$ and $\bar{R}$ are conjugate.

Factorise the first twenty primes of $\mathbb{Z}$ in $\mathbb{Z}[i]$. Do you see a pattern? Can you prove it?

- $2 = (1 + i)(1 - i)$ (conjugate primes), $5 = (2 + i)(2 - i)$, $7$ is prime, $11$ is prime, $13 = (2 + 3i)(2 - 3i)$, $17 = (4 + i)(4 - i)$, $19$ is prime, $23$ is prime, $29 = (5 + 2i)(5 - 2i)$, $31$ is prime, $37 = (6 + i)(6 - i)$, $41 = (5 + 4i)(5 - 4i)$, $43$ is prime, $47$ is prime, $53 = (7 + 2i)(7 - 2i)$, $59$ is prime, $61 = (6 + 5i)(6 - 5i)$, $67$ is prime, $71$ is prime, $73 = (8 + 3i)(8 - 3i)$.

- $2$ is special, otherwise the odd primes congruent to $1 \mod 4$ all split and the odd primes congruent to $3 \mod 4$ all stay prime.

(10) (For the set theorists) What is the transcendence degree of $\mathbb{R}$ over $\mathbb{Q}$?

If $X$ has infinite cardinality $\kappa$ then $\mathbb{Q}(X)[x]$ has size $\kappa$, and so there are $\kappa$ reals algebraic over $\mathbb{Q}(X)$. It follows that the transcendence degree is $2^{\kappa_0}$.

(11) (One to make you think. “Cheating” by consulting a book on algebraic number theory is fine, but think about it first). Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, by considering the equation $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Prove that each of the elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ is irreducible.

Note that for any integer $a$ and $b$, $|a + b\sqrt{-5}|^2 = a^2 + 5b^2$. We call this quantity the norm of $a + b\sqrt{-5}$. There are no elements of norms $2$ or $3$ and it follows by the multiplicativity of the norm that each of the elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ is irreducible.

Prove that every nonzero prime ideal is maximal.

In the complex plane the elements of $\mathbb{Z}[\sqrt{-5}]$ form a lattice (free additive subgroup of rank $2$). Any ideal forms a subgroup, and it is easy to see that any nonzero prime ideal must also have rank $2$. The quotient by a prime ideal is thus a finite ID, all finite IDs are fields, so all nonzero primes are maximal.

Find a representation of $(2)$ as a product of prime ideals.

If $(2)$ can be written as such a product, then $(2) \subseteq P$ for each prime factor $P$ and all such factors are maximal, so that $P$ corresponds to a maximal ideal of the quotient by $(2)$. The quotient by $(2)$ only has one such ideal and it follows that the only possible $P$ is the ideal generated by $2$ and $1 + \sqrt{-5}$. It is routine to check that $(2) = (2, 1 + \sqrt{-5})^2$. 