Problem 1. We proved in class the following result

Theorem 1. *Let R be a commutative unital ring and let $a \in R$ be an element which is not a zero divisors (so the sequence $a, a^2, a^3, ...$ does not contain 0). The set of ideals of R which are disjoint with the set $\{a, a^2, a^3, ...\}$ contains maximal elements, (i.e. ideals which are not contained in any larger ideal of this set) and any such ideal is prime.*

Use this theorem to prove that in a commutative unital ring the intersection of all prime ideals is equal to the nilradical (see problem 1 of homework 19 for definition, Problem 2 b) from homework 20 can be useful).

Solution: By Problem 2 b) from homework 20, if r is nilpotent and P is a prime ideal then $r \in P$. This proves that the nilradical N is contained in every prime ideal, hence in the intersection of all prime ideals. Suppose now that a is not nilpotent. By the theorem from class cited above, there exists a prime ideal Q which is disjoint form $a, a^2, ...$ In particular, $a \notin Q$ and therefore a does not belong to the intersection of all prime ideals. We showed that every element from N belongs to the intersection of all prime ideals and no element outside of N bolongs the intersection of all prime ideals. This means that N is equal to the intersection of al prime ideals of R.

Problem 2. Let R be an integral domain. Suppose that $0 \neq a \in R$ is such that aR is a prime ideal. Prove that a is irreducible.

Remark. The ring R is not considered a prime ideal, i.e. prime ideals are proper (I might have forgotten to add this in the definition).

Solution: Suppose that aR is a prime ideal. If $a = xy$ then $xy \in aR$. Since aR is prime, we have either $x \in aR$ or $y \in aR$. In the former case, $x = az$ for some $z \in R$ and therefore $a = azy$ so $zy = 1$ and y is invertible. In the latter case, we see simlarly that x is invertible. This shows that a is irreducible.

Problem 3. Consider the ring $R = \mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$, where n is an integer which is not a square (so $\sqrt{n}$ is not rational).

a) Define a map $f : R \longrightarrow R$ by $f(a + b\sqrt{n}) = a - b\sqrt{n}$. Prove that f is an isomorphism.

b) Consider the map $N : R \longrightarrow \mathbb{Z}$ defined by $N(a+b\sqrt{n}) = a^2 - nb^2$. Prove that $N(xy) = N(x)N(y)$ for all $x, y \in R$. Prove that $x \in R$ is invertible iff $N(x) = \pm 1$. Prove that if $|N(x)|$ is a prime number then x is irreducible.

c) Prove that $4+i$ is irreducible in $\mathbb{Z}[i]$. Prove that the only invertible elements of $\mathbb{Z}[i]$ are $1, -1, i, -i$.

d) Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many invertible elements. **Hint:** Consider $1+\sqrt{2}$. Note that product of invertible elements is invertible.

Solution: a) To see that f is a homomorphism note that

$$f((a+b\sqrt{n})+(c+d\sqrt{n})) = f((a+c)+(b+d)\sqrt{n}) = (a+c)-(b+d)\sqrt{n} =$$

$$= (a-b\sqrt{n})+(c-d\sqrt{n}) = f((a+b\sqrt{n}))+f((c+d\sqrt{n}))$$

and

$$f((a+b\sqrt{n})(c+d\sqrt{n})) = f((ac+nbd)+(bc+ad)\sqrt{n}) = (ac+nbd)-(bc+ad)\sqrt{n} =$$

$$= (a-b\sqrt{n})+(cd\sqrt{n}) = f((a+b\sqrt{n}))f((c+d\sqrt{n})).$$

Note now that $f(f((a+b\sqrt{n})) = f((a-b\sqrt{n}) = (a+b\sqrt{n})$, i.e. $f \circ f$ is the identity, so f its own inverse. Thus f is a bijection and therefore an isomorphism.

b) The first statement follows from the simple observation that $N(x) = xf(x)$ for all $x \in R$, where f is the isomorphism from a). Indeed, we have

$$N(xy) = xyf(xy) = xyf(x)f(y) = xf(x)yf(y) = N(x)N(y).$$

If $N(x) = \pm 1$ then $xf(x) = \pm 1$ so x is invertible. Conversely, assume that x is invertible. Then $xy = 1$ for some $y \in R$ and therefore

$$1 = N(1) = N(xy) = N(x)N(y).$$

Since both $N(x)$, $N(y)$ are integers, we must have $N(x) = \pm 1$.

Suppose now that $|N(x)|$ is a prime number. If $x = st$ for some $s, t \in R$, then $|N(x)| = |N(st)| = |N(s)||N(t)|$. But $|N(x)|$ is a prime number and $|N(s)|$, $|N(t)|$ are integers, so one of $|N(s)|$, $|N(t)|$ must be equal to 1. By our previous observation, this means that one of s, t is invertible. Thus x is irreducible.

c) We apply b) (Recall that $i = \sqrt{-1}$, i.e. $n = -1$ in this case). We have $N(4 + i) = 16 + 1 = 17$ is a prime, so $4 + i$ is irreducible. Also $a + bi$ is invertible iff $N(a + bi) = a^2 + b^2 = \pm 1$. Since a, b are integers, this holds only for $a = \pm 1$ and $b = 0$ or $a = 0$, $b = \pm 1$. Thus the only invertible elements are $1, -1, i, -i$.

d) Note that $(1+\sqrt{2})(-1+\sqrt{2}) = 1$. This shows that $1+\sqrt{2}$ is invertible in $\mathbb{Z}[\sqrt{2}]$. It follows that $(1+\sqrt{2})^m$ is invertible for every integer m. Since $1+\sqrt{2} > 1$, all the numbers $(1+\sqrt{2})^m$, $m \in \mathbb{Z}$, are different so we have infinitely many invertible elements.

Remark. It can be proved that the numbers $\pm(1+\sqrt{2})^m$, $m \in \mathbb{Z}$ are the only invertible elements of $\mathbb{Z}[\sqrt{2}]$.