Solutions to Homework 7

1. (a)

ideals	elements
$J \subset I$	$a \mid b$
$I + J = K$	$\gcd(a, b) = c$
$I \cap J = K$	$\mathrm{lcm}(a, b) = c$
$IJ = K$	$ab = c$
I is prime	a is prime
$I = J$	a and b differ by a unit
$I = R$	a is a unit

(b) To what extent can this analogy be made precise?

Solution: Let's work in a commutative ring, so it is reasonable to write things like $a \mid b$.

- If $I = (a)$ and $J = (b)$, then $J \subseteq I$ if and only if $a \mid b$.
- $\gcd(a, b) = c$ means that $c \mid a$, and $c \mid b$, and if $d \mid a$ and $d \mid b$ then $d \mid c$. For ideals, the analogue is an ideal K such that $I \subset K$, and $J \subset K$, and if $I, J \subset L$ then $K \subset L$. The ideal $K = I + J$ satisfies this.

  Let $I = (a)$ and $J = (b)$; then we can say that if $I + J = (a, b)$ is a principal ideal, say $I + J = (c)$, then $c = \gcd(a, b)$. Observe, however, that in $\mathbb{Z}[x]$ we have $\gcd(2, x) = 1$, but $(2, x)$ is not a principal ideal, and in particular is not (1). Or in $\mathbb{Z}[\sqrt{-5}]$ we have $\gcd(2, 1 + \sqrt{-5}) = 1$, but $(2, 1 + \sqrt{-5})$ is not a principal ideal, and in particular is not (1).
- $\mathrm{lcm}(a, b) = c$ means that $a \mid c$, and $b \mid c$, and if $a, b \mid d$ then $c \mid d$. For ideals, the analogue is an ideal K such that $K \subset I$, and $K \subset J$, and if $L \subset I$ and $L \subset J$ then $L \subset K$. The ideal $K = I \cap J$ satisfies this.

  Let $I = (a)$ and $J = (b)$; then we can say that if $I \cap J$ is a principal ideal, say $I \cap J = (c)$, then $c = \mathrm{lcm}(a, b)$. On the

other hand, in $\mathbb{Z}[\sqrt{-5}]$ one can show that $(2) \cap (1+\sqrt{-5}) = (6, 2+2\sqrt{-5})$, which is not principal, and that $\operatorname{lcm}(2, 1+\sqrt{-5})$ does not exist.

- If $I = (a)$ and $J = (b)$, then $IJ = (ab)$.
- If $I = (a)$, then I is a prime as an ideal if and only if a is prime as an element. Indeed, to say that a is prime means that $a \mid bc$ implies $a \mid b$ or $a \mid c$, and to say that I is prime means that $bc \in I$ implies $b \in I$ or $c \in I$.

  Later we will see that if I is prime and $JK \subset I$ then $J \subset I$ or $K \subset I$.
- In an integral domain, if $I = (a)$ and $J = (b)$, then $I = J$ if and only if there is a unit $u \in R$ such that $a = ub$.
- We have $(a) = (1)$ if and only if 1 is a multiple of a, which is true if and only if a is a unit.

2. Let R be a commutative ring. Show that $r \in R$ is prime if and only if R/r is an integral domain.

   Solution: Observe that for $a \in R$, we have $\bar{a} = 0$ in R/r if and only if $r \mid a$. Also observe that every element of R/r can be written as $\bar{a}$ for some $a \in R$.

   Now we see that the following are equivalent:

   - r is prime.
   - For $a, b \in R$, if $r \mid ab$ then $r \mid a$ or $r \mid b$.
   - For all $a, b \in R$, if $\overline{ab} = 0$ then $\bar{a} = 0$ or $\bar{b} = 0$.
   - For all $\bar{a}, \bar{b} \in R/r$, if $\bar{a}\bar{b} = 0$ then $\bar{a} = 0$ or $\bar{b} = 0$.
   - R/r is an integral domain.

3. Show that for a prime $p \in \mathbb{Z}$, the following are equivalent:

   (a) p can be written as $x^2 + y^2$ for $x, y \in \mathbb{Z}$.

   (b) p is not prime in $\mathbb{Z}[i]$.

   (c) $\mathbb{Z}[i]/p$ is not an integral domain.

   (d) $\mathbb{Z}_p[x]/(x^2+1)$ is not an integral domain.
   Hint: Consider $\mathbb{Z}[x]/(p, x^2+1)$. In lecture we showed that for a commutative ring R and two elements $r_1, r_2 \in R$, we have $(R/r_1)/\bar{r}_2 \cong R/(r_1, r_2)$.

(e) $x^2 + 1$ is not prime in $\mathbb{Z}/p$.

(f) -1 is a square mod p: that is, there is an $n \in \mathbb{Z}$ with $n^2 \equiv -1 \pmod{p}$.

Solution:

- $(a) \Leftrightarrow (b)$. First recall that $\mathbb{Z}[i]$ is a principal ideal domain, so an element is prime if and only if it is irreducible.

  Suppose that $p = x^2 + y^2 = (x + iy)(x - iy)$. We have $|x \pm iy|^2 = p \neq 1$, so $x \pm iy$ is not a unit, so p is reducible in $\mathbb{Z}[i]$. Conversely, suppose p is reducible in $\mathbb{Z}[i]$, say $p = zw$. Taking norms of both sides, we have $p^2 = |z|^2|w|^2$. Since z and w are not units, we have $|z|^2 \neq 1$ and $|w|^2 \neq 1$, so we must have $|z|^2 = p$ and $|w|^2 = p$. Write $z = x + iy$; then $|z|^2 = p$ becomes $x^2 + y^2 = p$.

- $(b) \Leftrightarrow (c)$ is immediate from problem 2.

- $(c) \Leftrightarrow (d)$: I claim that

  $$Z[i]/p \cong \mathbb{Z}[x]/(p, x^2 + 1) \cong \mathbb{Z}_p[x]/(x^2 + 1),$$

  so one is an integral domain if and only if the other one is. For the first isomorphism, apply the hint with $r_1 = x^2 + 1$ and $r_2 = p$, and recall that $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i]$. For the second isomorphism, apply the hint with $r_1 = p$ and $r_2 = x^2 + 1$, and recall that $\mathbb{Z}[x]/p \cong \mathbb{Z}_p[x]$, as we saw in lecture.

- $(d) \Leftrightarrow (e)$ is immediate from problem 2.

- $(e) \Leftrightarrow (f)$: First recall that $\mathbb{Z}_p[x]$ is a principal ideal domain, so $x^2 + 1$ is prime if and only if it is irreducible. Also recall that the units in $\mathbb{Z}_p[x]$ are just (non-zero) constant polynomials.

  If there is an $n \in \mathbb{Z}$ with $n^2 \equiv -1 \pmod{p}$, then we have

  $$(x + \bar{n})(x - \bar{n}) = x^2 + 1$$

  in $\mathbb{Z}_p[x]$, so $x^2 + 1$ is reducible. Conversely, if $x^2 + 1$ is reducible, say $x^2 + 1 = (x + \bar{m})(x + \bar{n})$ for some $m, n \in \mathbb{Z}$, then we have $m + n \equiv 0 \pmod{p}$ and $mn \equiv 1 \pmod{p}$. Thus $n \equiv -m \pmod{p}$, so $n^2 \equiv -mn \equiv -1 \pmod{p}$.