1

1.a

$\ker \varphi_a = \{x \in R \mid ax = 0\}$. R is an integral domain, so since $a \neq 0$, $ax = 0$ means that $x = 0$, so $\ker \varphi_a = \{0\}$, thus φ_a is injective, and since R is finite, this means that φ_a is also surjective, so φ_a is bijective.

Let $x, y \in R$. $\varphi_a(x + y) = a(x + y) = ax + ay = \varphi_a(x) + \varphi_a(y)$, so φ_a is a homomorphism. It is bijective, thus an isomorphism, and $\operatorname{Im} \varphi_a = R$, thus it is an automorphism, as desired.

1.b

Let $a \in R$, $a \neq 0$. Since φ_a is a bijection, it has an inverse, φ_a^{-1}. Consider φ_a^{-1}. $1 = \varphi_a(\varphi_a^{-1}(1)) = a\varphi_a^{-1}(1)$, so $\varphi_1^{-1}(1) = a^{-1}$. Thus any $0 \neq a \in R$ has an inverse, so R is a field.

2

$(a) \implies (b)$: $y = ux$, so $x \mid y$. u is a unit, so since $y = ux$, $x = u^{-1}y$, hence $y \mid x$.

$(b) \implies (c)$: We know that $a \mid b \iff b \in \langle a \rangle$, so $y \in \langle x \rangle$ and $x \in \langle y \rangle$. $y \in \langle x \rangle$, so $\langle y \rangle \subseteq \langle x \rangle$, and $x \in \langle y \rangle$, so $\langle x \rangle \subseteq \langle y \rangle$. Thus $\langle x \rangle = \langle y \rangle$.

$(c) \implies (a)$: $y \in \langle y \rangle$, and $\langle y \rangle = \langle x \rangle$, so $y \in \langle x \rangle$. Thus $y = ux$ for some $u \in R$. Similarly, $x \in \langle y \rangle$, so $x = vy$ for some $v \in R$. Then $y = u(vy) = (uv)y$, so $uv = 1$, thus u is a unit.

3

3.a

J is an ideal of R_P, so for any $\frac{i}{j} \in J$, $\frac{a}{b} \in R_P$, $\frac{ai}{bj} \in J$. Let $i \in I$, $r \in R$. $1 \notin P$ since P is prime, so $\frac{r}{1} \in R_P$. We know that there is a $p \in P$ such that $\frac{i}{p} \in J$, so $\frac{r}{1} \cdot \frac{i}{p} = \frac{ri}{p} \in J$, then $ri \in I$, so since i and r were arbitrary, I is an ideal of R.

3.b

Let J be an ideal of R_P. Let I be the set of numerators of elements of J. We just showed that I is an ideal of R. Let $I = \langle a \rangle$. Then any element of J has the form $\frac{ra}{b}$, $b \notin P$ for some $r \in R$. $\frac{ra}{b} = \frac{r}{b} \cdot \frac{a}{1}$, so $J = \langle \frac{a}{1} \rangle$, thus R_P is a PID.

4

4.a

Let $a_1 \in R$ be a nonzero non-unit, and assume for a contradiction that a_1 cannot be written as a product of irreducibles. a_1 is not irreducible, otherwise $a_1 = a_1$ would be a_1 written as a product of irreducibles. So $a_1 = bc$, for non-units $b, c \in R$. b or c must not be able to be written as a product of irreducibles (otherwise we could use their decomposition into irreducibles to write a_1 as a product of irreducibles) so WLOG b cannot be written as a product of irreducibles. Let $a_2 = b$. $a_1 \in \langle a_2 \rangle$, so $\langle a_1 \rangle \subseteq \langle a_2 \rangle$. $\langle a_1 \rangle \neq \langle a_2 \rangle$, otherwise $a_2 = ra_1$, then $a_1 = (ra_1)c = (rc)a_1$, so $rc = 1$, but c was not a unit. We can continue this process to construct an infinite chain $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$, a contradiction, so a_1 can be written as a product of irreducibles, as desired.

4.b

Let $r = p_1 \cdots p_k$. If $d \mid r$, d irreducible, then there is some $q \in R$ such that $r = qd$, so $qd = p_1 \cdots p_k$. $p_1 \cdots p_k$ is unique up to order and units, so we can assume $ud = pk$, $vq = p_1 \cdots p_{k-1}$ for some units $u, v \in R$. So any divisor d of r must be one of $p_1, \ldots, p_k$ multiplied by a unit, thus r has, up to units, k divisors.

So any element $r \in R$ has a finite number of divisors up to units. That is to say, any element dividing r lies in one of finitely many principal ideals $\langle p_1 \rangle, \ldots, \langle p_k \rangle$.

Now suppose for a contradiction that there exists a sequence $a_1, a_2, \ldots \in R$ such that $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$. Consider the element $s = a_1 \cdot a_2 \cdot \ldots$. s has only finitely many divisors, so somewhere in the sequence $\langle a_i \rangle$ must become equal to $\langle a_{i+1} \rangle$, a contradiction, so no such sequence exists, and R thus has the $\heartsuit$ property.

5

R is a PID, so $\langle a, b\rangle = \langle d\rangle$ for some $d \in R$. $a, b \in \langle a, b\rangle$, so $a, b \in \langle d\rangle$, and thus $d \mid a$ and $d \mid b$. We claim that d is a gcd of a and b.

Let $q \in R$ such that $q \mid a$ and $q \mid b$. Then $a = nq$ and $b = mq$ for some $n, m \in R$. $\langle d\rangle = \langle a, b\rangle$, so $d \in \langle a, b\rangle$, thus $d = xa + yb$ for some $x, y \in R$. Then $d = x(nq) + y(mq) = (xn + ym)q$, so $q \mid d$. Thus d is a gcd of a and b.

Now let c be any arbitrary gcd of a and b. We know, since $d \mid a$ and $d \mid b$, that $d \mid c$, so $c \in \langle d\rangle = \langle a, b\rangle$, as desired.

6

6.a

Let $I = \langle a_1, \ldots, a_k\rangle \subseteq R$ be a finitely generated ideal. We prove I is principal by induction on k:

This is true by definition when $k = 1$, and when $k = 2$, let $r \in \langle a, b\rangle$, d a gcd of a and b. $r = xa + yb$ for some $x, y \in R$, and $d \mid a$ and $d \mid b$, so $a = nd$, $b = md$ for some $n, m \in R$. Thus $r = x(nd) + y(md) = (xn + ym)d$, so $r \in \langle d\rangle$. Thus $\langle a, b\rangle \subseteq \langle d\rangle$. Now let $r \in \langle d\rangle$. Then $r = zd$ for some $z \in R$. $d \in \langle a, b\rangle$, so $d = ia + jb$ for some $i, j \in R$. So $r = z(ia + jb) = (zi)a + (zj)b \in \langle a, b\rangle$, so $\langle d\rangle \subseteq \langle a, b\rangle$, and so $\langle a, b\rangle = \langle d\rangle$, and thus $\langle a, b\rangle$ is principal.

Assume $\langle a_1, \ldots, a_k$ is principal for any $k \leq n$, and consider $\langle a_1, \ldots, a_{n+1}\rangle$. Let $r = c_1a_1 + \cdots + c_{n+1}a_{n+1} \in \langle a_1, \ldots, a_{n+1}\rangle$. By our hypothesis, $\langle a_1, \ldots, a_n\rangle$ is principal, say generated by d. Then $r - c_{n+1}a_{n+1} \in \langle d\rangle$, so $r \in \langle d, a_{n+1}\rangle$. Again by our hypothesis, $\langle d, a_{n+1}\rangle$ is principal, as desired. So by induction, every finitely generated ideal of R is principal.

6.b

Assume for a contradiction that $I \subseteq R$ is a non finitely generated ideal, say $I = \langle a_1, a_2, \ldots\rangle$. Every finitely generated ideal of R is principal, so $\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \subsetneq \cdots$ is a sequence of principal ideals, a contradiction since R is a UFD, and therefore has the ♡ property. So no such I exists, and thus every ideal is finitely generated, and thus principal. So R is a PID, as desired.