In the UFD problems below it will be helpful to set \( \alpha = \prod p_i^{a_i}, \beta = \prod p_i^{b_i}, \gamma = \prod p_i^{c_i} \).

1. Let \( D \) be a Unique Factorization Domain. Let \( 0 \neq \alpha, \beta, \gamma \in D \). Define the least common multiple \( \text{lcm}(\alpha, \beta) \) by

\[
\kappa = \text{lcm}(\alpha, \beta) = \frac{\alpha \beta}{\gcd(\alpha, \beta)}
\]

(a) Show that \( \alpha \mid \kappa \) and \( \beta \mid \kappa \).

Solution: Then \( \kappa = \prod \pi_i^{d_i} \) where \( d_i = a_i + b_i - \min(a_i, b_i) = \max(a_i, b_i) \) Then \( a_i, b_i \leq \max(a_i, b_i) \)

(b) Show that if \( \alpha \mid \lambda \) and \( \beta \mid \lambda \) then \( \kappa \mid \lambda \).

Solution: Writing \( \lambda = \prod \pi_i^{e_i}, \ a_i, b_i \leq e_i \) so \( e_i \leq d_i \).

2. Continuing, in a PID \( D \).

(a) Let \( \kappa = \gcd(\gcd(\alpha, \beta), \gamma) \). Show that \( \kappa \) doesn’t depend on the order of \( \alpha, \beta, \gamma \). We call this \( \kappa = \gcd(\alpha, \beta, \gamma) \).

Solution: This will be the min of the three exponents

(b) Let \( \kappa = \text{lcm}(\text{lcm}(\alpha, \beta), \gamma) \). Show that \( \kappa \) doesn’t depend on the order of \( \alpha, \beta, \gamma \). We call this \( \kappa = \text{lcm}(\alpha, \beta, \gamma) \). (This extends to any number of variables.)

Solution: This will be the max of the three exponents

(c) Show

\[
\gcd(\text{lcm}(\alpha, \beta), \text{lcm}(\alpha, \gamma), \text{lcm}(\beta, \gamma)) = \text{lcm}(\gcd(\alpha, \beta), \gcd(\alpha, \gamma), \gcd(\beta, \gamma))
\]

Solution: The first expression gives the max of the three pairwise mins (of \( a_i, b_i, c_i \)) and the second gives the min of the three pairwise maxes. In both cases it is the middle of the three exponents.

3. Let \( R \) be a ring, \( I \subset R \) and ideal, \( a \in R \). Set

\[
J = \{ i + ra : i \in I, r \in R \}
\]
(a) Let \( K \subset R \) be an ideal. Assume \( I \subset K \) and \( a \in K \). Prove \( J \subset K \).

**Solution:** Let \( \alpha = i + ra \in J \). As \( i \in I, i \in K \). As \( a \in K, ra \in K \), so \( i + ra \in K \).

(b) Prove that \( J \) is an ideal.

**Solution:** We need to show \( 0 \in J \), \( \alpha \in J \Rightarrow -\alpha \in J \), \( \alpha, \beta \in J \Rightarrow \alpha + \beta \in J \) and \( \alpha \in J, s \in R \Rightarrow sa \in J \). Let \( \alpha, \beta \in J \). We can write \( \alpha = i_1 + r_1a, \beta = i_2 + r_2a \). Then \( \alpha + \beta = (i_1 + i_2) + (r_1 + r_2)a \) so \( \alpha + \beta \in J \).

Because of the above we refer to \( J \) as the *extension* of \( I \) by \( a \).

4. In \( Z[i] \) let \( \overline{\pi} \) denote the complex conjugate and \( \sim \) denote associate.

(a) Set \( \pi = 1 + i \). Show that \( \pi \sim \overline{\pi} \).

**Solution:** \( 1 - i = (-i)(1 + i) \).

(b) Show that \( \pi = 1 + i \) is the only nonreal prime in \( Z[i] \) with \( \pi \sim \overline{\pi} \).

**Solution:** If \( \pi \) is at angle \( \theta \) then \( \overline{\pi} \) is at angle \( -\theta \), so \( \theta, -\theta \) differ by a multiple of \( \pi/2 \). Adding \( \pi/2 \) to the angle we still have an associate so there are only two cases. We could have \( \theta = 0 \), but then \( \pi \) is real. Or we can have \( \theta = \pi/4 \). Then, looking at the geometry, \( \pi \) would be a multiple of \( 1 + i \). All \( n(1 + i) \) with \( n > 1 \) are nonprime since \( 1 + i \) is a divisor. Hence the only possibility is \( \pi = 1 + i \).

(c) Let \( m, n \in Z \), nonzero. Show that \( \gcd(m, n) \), as defined in \( Z \), is the same as \( \gcd(m, n) \), defined in \( Z[i] \).

**Solution:** Let \( a = \gcd(m, n) \) in \( Z \). Then \( a|m \) and \( a|n \) and there exist \( x, y \in Z \) with \( a = mx + ny \). But then the same holds for this \( a \) in \( Z[i] \). We showed in class that these two properties imply that we have the gcd. (Note: This argument works for any two PIDs, \( R \subset R^* \). The value of the gcd for elements in the smaller PID does not change. However, primality can and often does change.)

5. By \( C^* \) we mean \( C \setminus \{0\} \), the nonzero complex numbers. Here we examine \( C^*, \cdot \), the group under multiplication. Let \( S \) be the set of solutions to the equation \( z^{12} = 1 \).

(a) Draw a nice picture of \( S \) on the complex plane \( C \).

**Solution:** It should look like the hours of a clock.
(b) For each $z \in S$ marked above, give the minimal positive integer $s$ with $z^s = 1$.

Solution: Set $\epsilon = e^{2\pi i/12}$, one twelfth around the circle, so that $\epsilon^j$ is at “$j$ o’clock.” Then the roots are $z = \epsilon^j$, $0 \leq j < 11$. $j = 0$ is $z = 1$ with $s = 1$, $j = 6$ is $z = -1$ with $s = 2$, $j = 4, 8$ give $z = \omega, \omega^2$ where $\omega = (-1 + i\sqrt{3})/2$ is a cube root of unity. For them, $s = 3$. $j = 3, 9$ give $z = i, -i$ with $s = 4$. $j = 2, 10$ give $s = 6$ (e.g. $(\epsilon^2)^6 = \epsilon^{12} = 1$. Finally, $j = 1, 5, 7, 11$ give $s = 12$.

(c) Prove that $S$ is a subgroup of $C^*$.

Solution: One approach is that $1 \in S$; $a, b \in S$ imply $(ab)^{12} = a^{12}b^{12} = 1$ so $ab \in S$; $a \in S$ implies $(a^{-1})^{12} = (a^{12})^{-1} = 1^{-1} = 1$ so $a^{-1} \in S$. Another is to note that $S$ under multiplication is isomorphic to $Z_{12}$ under addition by identifying $\epsilon^j$ with $j$.

(d) Prove that $S$ is the only subgroup of $C^*$ with (precisely) twelve elements.

Solution: If $T$ were a subgroup with 12 elements then by Lagrange’s Theorem $w^{12} = 1$ for each $w \in T$, so $T \subseteq S$. As they both have 12 elements, $T = S$.

6. Set $Z[\sqrt{-2}] = \{a + b\sqrt{-2}\}$. This is a Euclidean Domain (a nice exercise but not requested) with $d(\alpha) = |\alpha|^2 = a^2 + 2b^2$. Assuming that show:

(a) If $d(\alpha)$ is an integer prime then $\alpha$ is a prime.

Solution: If $\alpha = \beta\gamma$ then $d(\alpha) = d(\beta)d(\gamma)$ so $d(\beta) = 1$ (or $d(\gamma) = 1$) so $\beta$ is a unit.

(b) If $p$ is an integer prime and there $p = x^2 + 2y^2$ has an integer solution then $p$ is not a prime in $Z[\sqrt{-2}]$.

Solution: $p = (x + y\sqrt{-2})(x - y\sqrt{-2})$

(c) If $p$ is an integer prime and there $p = x^2 + 2y^2$ has no integer solution then $p$ is a prime in $Z[\sqrt{-2}]$.

Solution: If $p = \beta\gamma$ then $p^2 = d(p) = d(\beta)d(\gamma)$ so $d(\beta) = p$, but writing $\beta = x + y\sqrt{-2}$ we would have $p = x^2 + 2y^2$. 