Exercises 3, 7, 8, 10 pp. 277-279.

Problem 3. Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such a element exists) is a unit.

Proof. Suppose $a \in R$ and $N(a) = m$. Divide 1 by a using the Euclidean division to obtain $1 = qa + r$, where $N(r) = 0$ or $N(r) < N(a)$. By the minimality of m, only the first case is possible. Thus $r = 0$, and we see that $1 = qa$; hence a is a unit.

Since 0 is the minimum natural number, if there were a nonzero element $a \in R$ such that $N(a) = 0$, then by the above argument it would be a unit. □

Problem 7. Find a generator for the ideal $(85, 1+13i)$ in $\mathbb{Z}[i]$, i.e., a greatest common divisor of 85 and $1+13i$, by the Euclidean Algorithm. Do the same for the ideal $(47-13i, 53+56i)$.

Proof. Just compute:

For $(85, 1 + 13i)$:

$$\begin{aligned}
\frac{85}{1+13i} &= \frac{1-13i}{2} \Rightarrow p = 0, q = -6 \\
85 &= -6i * (1 + 13i) + r = 78 + -6i + r \Rightarrow r = 7 + 6i \\
\frac{1+13i}{7+6i} &= \frac{(1+13i)(7-6i)}{85} = \frac{7+91i-6i+78}{85} = \frac{85+85i}{85} = 1+i
\end{aligned}$$

Hence $(85, 1 + 13i) = (1 + i)$.

For $(47 - 13i, 53 + 56i)$: Let $a = 47 - 13i, b = 53 + 56i$. Then $N(a) = 2378, N(b) = 5945$, so

$$\begin{aligned}
\frac{b}{a} &= \frac{53+56i}{47-13i} = \frac{(53+56i)(47+13i)}{2378} = \frac{1763+3321i}{2378} \\
&\Rightarrow p = 1, q = 1 \Rightarrow b = (1 + i)a + r \\
r &= (53 + 56i) - (1 + i)(47 - 13i) = -7 + 22i, N(r) = 533 \\
\frac{a}{r} &= \frac{47-13i}{-7+22i} = -\frac{(47-13i)(7+22i)}{533} = -\frac{615+943i}{533} \\
&\Rightarrow p = -1, q = -2 \Rightarrow a = -(1 + 2i)r + r_1 \\
r_1 &= (47 - 13i) + (1 + 2i) * (-7 + 22i) = -4 - 5i, N(r_1) = 41 \\
\frac{r}{r_1} &= \frac{-7+22i}{-4-5i} = \frac{(7-22i)(4-5i)}{41} = -\frac{82+123i}{41} = -2-3i
\end{aligned}$$

Hence $(47-13i, 53+56i) = (-2-3i) = (2+3i)$. $\square$

Problem 8. Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field with associated quadratic integer ring $\mathcal{O}$ and field norm N as in Section 7.1.

(a) Suppose D is $-1, -2, -3, -7$ or -11. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N. [Modify the proof for $\mathbb{Z}[i]$ $(D = -1)$ in the text.]

(b) Suppose that $D = -43, -67$ or -163. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm. [Apply the same proof as for $D = -19$ in the text.]

Proof. We proceed with each separately.

(a) For this proof we follow the same steps as in the text. Let $F = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}_F$ be its field of integers. Let $\alpha, \beta \in \mathcal{O}_F$ where $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$. Now as in the text, we choose $p + qi$ such that the norm of the distance between $p + qi$ and α/β is minimized. (In the case where $D = -1$, this just means choosing the closest integer values for p and q. Then we have $N(\theta) = N(\alpha - (p + qi)\beta) \leq 1/2$.)

In the case where $D = -2$, not much changes; the imaginary part of θ is bounded instead by $\sqrt{2}/2$. Hence $N(\theta) = N(\alpha - (p + qi)\beta) \leq 1/4 + 1/2 = 3/4$.

Now we consider the cases $D = -3, -7, -11$. These all satisfy $D \not\equiv 3 \bmod 4$, so the integers are given by $a + \frac{1+\sqrt{D}}{2}b$. Again, we want to find the minimum distance between α/β and some point in $\mathcal{O}_F$. From a geometric point of view, $\mathcal{O}_F$ looks like a lattice on the complex plane. Specifically, $\mathcal{O}_F$ looks like a triangular lattice because of the $\frac{1+\sqrt{D}}{2}$ terms we use to generate our elements. (This is opposed to $\mathbb{Z}[i]$, whose lattice just looks square.)

From a geometric point of view, then, we are trying to find minimum distance between a tiling of triangles and a point. This is equivalent to finding the minimum distance between a point and the vertices of the triangle region it sits in. And this distance is bounded by the circumradius, the longest distance any point can have from all three vertices at the same time.

It is a well-known formula that the circumradius of a triangle of given by $abc/4A$, where a, b, c are the sides of the triangle and A is the area. In our case, the triangle has side lengths 1, $\sqrt{1 + |D|}/2$, $\sqrt{1 + |D|}/2$ and area $\frac{1}{2}(1)(\sqrt{|D|}/2)$. Hence $R = (1+|D|)/4\sqrt{D}$.

Returning back to the problem, this means that the minimum norm between α/β and some element of $\mathcal{O}_F$ is bounded by $(1 + |D|)^2/16|D|$. For $D = -3, -7, -11$, this value is less than 1. Hence again $N(\theta) < 1$.

Putting all the cases together, we have $\alpha = (p+qi)\beta + \gamma$ for some well chose $p+qi$ such that $\gamma = \beta\theta$. Since $N(\theta) < 1$, we have $N(\gamma) = N(\beta)N(\theta) < N(\beta)$. And so we're done.

(b) Again we follow the text. Note that the minimum values of N on R are 1 and 4, given by ± 1 and ± 2, since $43/4, 67/4, 163/4 \geq 5$.

Choosing $x = 2$, we must have u must divide 2 or 3. As in the text, we deduce that $u = \pm 2$ or $u = \pm 3$. Then it is clear that u does not divide $\frac{1+\sqrt{D}}{2}$. Hence there are no universal side divisors, and R is not an Euclidean domain.

□

Problem 10. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$.

Proof. Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a PID; thus $I = (\alpha)$ for some nonzero α. Using the Euclidean division, every element $b \in \mathbb{Z}[i]$ can be written as $q\alpha + r$, and hence all the ideals $(\alpha) + r$ are represented $\{r \mid N(r) < N(\alpha)\}$. There are only a finite amount of integer solutions to $a^2 + b^2 < N(\alpha)$, so there are only a finite number of cosets of the form $(\alpha) + r$. Hence $\mathbb{Z}[i]/I$ is finite. □

Exercises 1, 3, 4, 5, 6 pp. 282-283.

Problem 1. Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal if and only if a greatest common divisor of a and b is 1 (in which case a and b are said to be *coprime* or *relatively prime*.)

Proof. We have (a) and (b) are comaximal iff $(a) + (b) = R = (1)$, which occurs iff the gcd of a and b is 1. So we're done. □

Problem 3. Prove that a quotient of a PID by a prime ideal is once again a PID.

Proof. Let R be a PID and P be a prime ideal of R. If $P = 0$, then $R/P \cong R$, which is a PID. Otherwise, P must be a maximal ideal of R, since every nonzero prime ideal in a PID is a maximal ideal. Then R/P is a field, and hence it is trivially a PID as well. □

Problem 4. Let R be an integral domain. Prove that if the following two conditions hold then R is a PID:

(i) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and

(ii) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1} \mid a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

Proof. Let $a_1 \in I$. If $(a_1) = R$, then we're done, otherwise, pick some $b_1 \in I - (a)$ and consider $(a_2) = (a_1, b_1)$. Now repeat this process: for any n, if $(a_n) = R$, then we're done; otherwise, pick some $b_n \in I - (a_n)$ and construct $(a_{n+1} = (a_n, b_n))$.

If this process terminates, then we will have $(a_n) = R$ for some n and hence I is principal. Furthermore, this process must terminate; if it did not, then we would have an strictly ascending chain $(a_1) \subset (a_2) \subset \ldots$, which contradicts condition (ii) $\square$

Problem 5. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 2+\sqrt{-5})$, and $I_3' = (3, 2-\sqrt{-5})$.

(a) Prove that I_2, I_3, and I_3' are nonprincipal ideals in R.

(b) Prove that the product of two nonprincipal ideals can be principal by showing that I_2^2 is the principal ideal generated by 2, i.e., $I_2^2 = (2)$.

(c) Prove similarly that $I_2 I_3 = (1-\sqrt{-5})$ and $I_2 I_3' = (1+\sqrt{-5})$ are principal. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.

Proof.

(a) First let us consider I_2: We claim that $I_2 = J_2 = \{a + b\sqrt{-5} \mid a \equiv b \bmod 2\}$. Indeed, $2, 1+\sqrt{-5} \in J_2$, so $I_2 \subseteq J_2$. For the other inclusion, if $a+b\sqrt{-5} \in J_2$, then either a and b are both even or both odd. If a and b are both even, then $a+b\sqrt{-5} = (a'+b'\sqrt{-5})(2) \in (2)$. Otherwise, $(a+b\sqrt{-5}) - (1+\sqrt{-5}) \in (2)$. So $a+b\sqrt{-5} \in (2, 1+\sqrt{-5})$ and $J_2 \subseteq I_2$. Hence $I_2 = J_2$, as desired.

Suppose for the sake of contradiction that $I_2 = (\alpha)$ is principal. We know $2 \in I_2$, so $\alpha \mid 2$. But then $N(\alpha) < N(2) = 4$ forces $\alpha = \pm 1$. This gives contradiction: $\pm 1 + 0i$ cannot be in I_2 since $\pm 1 \not\equiv 0 \bmod 2$.

Similarily, we can show that $I_3 = \{a + b\sqrt{-5} \mid a \equiv -b \bmod 3\}$ and $I_3' = \{a + b\sqrt{-5} \mid a \equiv b \bmod 3\}$. Then we can follow the above argument with 3 instead of 2 to reach contradiction for assuming that I_3 and I_3' are principal.

We conclude that I_2, I_3, and I_3' are all nonprincipal ideals.

(b) We prove both inclusions. First we show $I_2^2 \subseteq (2)$. Let $a+b\sqrt{-5}, c+d\sqrt{-5} \in I_2$, then $(a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-5bd)+(ad+bc)\sqrt{-5}$. Since $a \equiv b \bmod 2$ and $c \equiv d \bmod 2$, we have $ac \equiv -5bd \bmod 2$ and $ad \equiv bc \bmod 2$. So $(a+b\sqrt{-5})(c+d\sqrt{-5}) \in (2)$. We conclude that $I_2^2 \subseteq (2)$.

Now we have $(1+\sqrt{-5})(1-\sqrt{-5}), 2^2 \in I_2^2$, hence $(1+\sqrt{-5})(1-\sqrt{-5}) - 2^2 = 2 \in I_2^2$. Thus $(2) \subseteq I_2^2$, proving that $I_2^2 = (2)$.

(c) Again we prove both inclusions. Note that $(2+\sqrt{-5}) - (1+\sqrt{-5}) = 1$ and $1-\sqrt{-5}$ is both in I_2 and I_3, so we may write

$$\begin{aligned} 1-\sqrt{-5} &= (1-\sqrt{-5})((2+\sqrt{-5}) - (1+\sqrt{-5})) \\ &= (1-\sqrt{-5})(2+\sqrt{-5}) - (1-\sqrt{-5})(1+\sqrt{-5}) \\ &\in I_2I_3 + I_3I_2 \subseteq I_2I_3. \end{aligned}$$

Hence $(1-\sqrt{-5}) \subseteq I_2I_3$.

For the other inclusion, let $a+b\sqrt{-5} \in I_2I_3$. Then $a+bi \in I_2I_3 \subseteq I_2 \cap I_3$, so we know that $a \equiv -b \bmod 2, 3$. This implies $a \equiv -b \bmod 6$. This allows us to rewrite

$$a + b\sqrt{-5} \equiv a + b \equiv 6n \bmod (1-\sqrt{-5}).$$

But $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, so in fact $1-\sqrt{-5}$ divides $a+bi$! Hence $a+bi \in (1-\sqrt{-5})$; we conclude that $I_2I_3 = (1-\sqrt{-5})$.

The result for $I_2I_3' = (1+\sqrt{-5})$ holds similarily.

Now it is clear to see that $(I_2I_3)(I_2I_3') = I_2^2I_3I_3' = (1-\sqrt{-5})(1+\sqrt{-5}) = (6)$.

□

Problem 6. Let R be an integral domain and suppose that every *prime* ideal in R is principal. This exercise proves that every ideal of R is principal, i.e., R is a PID.

(a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]

(b) Let I be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let $I_b = (I, b)$ be the ideal generated by I and b, and define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subset I_b \subseteq J$ and $I_aJ = (\alpha\beta) \subseteq I$.

(c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_aJ$ is principal, a contradiction, and conclude that R is a PID.

Proof. We proceed with each separately:

(a) Consider the union of all non-principal ideals of R. Since R itself is principal, this union cannot be R, and hence strictly a subset of R. But the union is also an upper bound to all non-principal ideals, so we may apply Zorn's lemma to show that there is some maximal non-principal ideal in R.

(b) Let I be such a maximal non-principal ideal. Let $ab \in I$ and $a, b \notin I$. This forces I_a and I_b to be strictly greater than I, so they must be principal. Furthermore, note that if $r \in I$, then $rI_a \subseteq II_a \subseteq I$. Therefore $r \in I \subseteq J$. At the same time, $bI_a = b(I, a) = bI + b(a) \subseteq I + I \subseteq I$; hence $b \in J$. So we have $I \subset I_b \subseteq J$, implying that J is also principal. Set $I_a = (\alpha)$ and $J = (\beta)$. By the definition of J, we have $rI_a \subseteq I$ for all $r \in J$, so $JI_a = (\alpha\beta) \subseteq I$.

(c) Let $x \in I$. Then $I \subset I_a$ so $x = s\alpha$ for some $s \in R$. By definition, this means that $s \in J$. But this implies that $I \subseteq I_a J$, which is a principal ideal! Thus we we contradiction; R must be a PID.

$\square$

Exercises 6, 8 pp. 292-293.

Problem 6.

(a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

(c) Let $p \in \mathbb{Z}$ by a prime with $p \equiv 1 \bmod 4$ and write $p = \pi\overline{\pi}$ as in Proposition 18. Show that the hypotheses for the Chinese Remainder Theorem are satisfied and that $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are both fields of order p.

Proof.

(a) From Problem 10 above, the elements of $\mathbb{Z}[i]/(1+i)$ can be identified with the cosets $(1+i)+r$, where $N(r) < N(1+i) = 2$. This leaves only 0, ± 1, and $\pm i$ as choices for r. Furthermore, notice that the cosets generated by ± 1 and $\pm i$ are all equal to $(1+i)+1$. So there are only two distinct cosets $(1+i)$ and $(1+i)+1$, corresponding to two elements of $\mathbb{Z}[i]/(1+i)$. There is only one ring with two elements, namely $\mathbb{Z}_2 = \mathbb{F}_2$ the field of two elements, as desired.

(b) To see that $\mathbb{Z}[i]/(q)$ has q^2 elements, first focus on the group structure. Consider the map $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_q^2$ sending $a + bi \mapsto (a \bmod q, b \bmod q)$. This is clearly a group homomorphism. The kernel of φ are elements such $a \bmod q = b \bmod q = 0$, i.e.

$a + bi = q(a' + b'i) \in (q)$. Thus $\ker\varphi = (q)$ and the first isomorphism theorem gives $\mathbb{Z}[i]/(q) \cong \mathbb{Z}_q^2$ as groups. In particular, we conclude that $\mathbb{Z}[i]/(q)$ has order q^2.

Since $q \equiv 3 \bmod 4$, we know that (q) is prime. But $\mathbb{Z}[i]$ is a PID, so (q) is maximal; therefore $\mathbb{Z}[i]/(q)$ is a field.

(c) It suffices to show that π and $\overline{\pi}$ are comaximal. Indeed, let $\pi = a + bi$, so that $p = (a + bi)(a - bi) = a^2 + b^2$. So both $a, b \nmid p$. The ideal $(a + bi, a - bi)$ contains $a + bi + a - bi = 2a$. Since $p \neq 2$, there is some inverse x such that $2ax = 1$. Hence $(a + bi, a - bi) = (1)$, and π and $\overline{\pi}$ are comaximal. Thus

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$$

is a product of two fields of order p.

$\square$

Problem 8. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ and define the ideals $I_2 = (2, 1 + \sqrt{-5}), I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.

(a) Prove that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducibles in R, no two of which are associate in R, and that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R.

(b) Prove that I_2, I_3, and I_3' are prime ideals of R.

(c) Show that the factorizations in (a) imply the equality of ideals $(6) = (2)(3)$ and $(6) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Show that these two ideal factorizations give the same factorizations of the ideal as the product of prime ideals.

Proof.

(a) Let $r \in \{2, 3, 1 \pm \sqrt{-5}\}$. If $\alpha\beta = r$, then $N(\alpha)N(\beta) = N(r)$. But $N(r)$ can only be $4, 6$, or 9. Note that $a^2 + 5b^2 = 2, 3$ both have no solutions in the integers, one of $N(\alpha)$ or $N(\beta)$ must be equal to 1. Hence α or β is a unit, and r is irreducible.

Furthermore, since only $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ have the same norm, they may be associates. But $\frac{1+\sqrt{-5}}{1-\sqrt{-5}}$ is not in $\mathbb{Z}[\sqrt{-5}]$, so this fails. Hence $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R.

(b) It suffices to show that $\mathbb{Z}[\sqrt{-5}]/\{I_2, I_3, I_3'\}$ are integral domains. Indeed, from Problem 8.2.6 above, we know that there are only two types of elements in I_2: those with a, b both odd or both even. Hence $\mathbb{Z}[\sqrt{-5}]/I_2$ is the ring of two elements, which is trivially an integral domain.

For $\mathbb{Z}[\sqrt{-5}]/I_3$, we again know from Problem 8.2.6 above that there are 3 types of elements, so $\mathbb{Z}[\sqrt{-5}]/I_3$ is the ring of three elements, which is also trivially an integral domain. The same holds for $\mathbb{Z}[\sqrt{-5}]/I_3'$.

In any case, this shows that I_2, I_3, and I_3' are prime ideals.

(c) The equalities $(6) = (2)(3)$ and $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$ follow directly from $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. From Problem 8.2.6 above, we have $(2) = I_2^2$ and $(3) = I_3 I_3'$, while $(1-\sqrt{-5}) = I_2 I_3$ and $(1+\sqrt{-5}) = I_2 I_3'$. So clearly

$$(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5}) = I_2^2 I_3 I_3'.$$

$\square$