Prof. Dr. Özlem Imamoglu

Solutions Exercise sheet 1

1. Let R be a principal ideal domain.

(a) Show that every ascending chain of ideals, $I_1 \subseteq I_2 \subseteq \cdots$, eventually become stationary. Or in other words, there is a positive index n such that $I_k = I_n$ for all $k \geqslant n$.

(b) Show that every irreducible element is a prime element.

Solution: (a) Let $I = \cup I_i$. Then, if $a, b \in I$, we have that $a \in I_m$ and $b \in I_n$, for some m, n. Hence $a, b \in I_{\max\{m,n\}}$, so $a \pm b \in I_{\max\{m,n\}} \subset I$. Thus I is a subrgoup under addition. If $a \in I$ then $a \in I_n$ for some n, and since I_n is an ideal we have $ra \in I_n$ for all $r \in R$. Thus $ra \in I$ for all $r \in R$. Since R is a principal ideal domain, there exists $a_0 \in R$ with $I = (a_0)$. Now $b \in I$, so there exists a positive integer n_0 such that $a_0 \in I_{n_0}$. Thus $I = (a_0) \subset I_{n_0}$. Hence if $n \geqslant n_0$ then $I \subset I_{n_0} \subseteq I_n \subseteq I$. Hence $I_n = I_{n_0}$.

(b) Let $a \in R$ be irreducible and let $b, c \in R$ with $a \mid bc$. If $a \mid b$, then we are done. Suppose $a \nmid b$. Then if $u \mid a$, we have that either u is invertible or u is an invertible element times a, since a is assumed to be irreducible. Thus is u divides both a, b then u must be invertible. Hence if a doesn't divide b then a, b are relatively prime. Then the result will follow from the following claim:

Claim. Let a, b be non-zero relatively prime elements of R. Then if $a \mid bc$ with $c \in R$ then $a \mid c$.

Proof of claim. Since a, b are relatively prime, we can write an invertible element $u \in R$ as $u = as + bt$. Writing $p = s/u$ and $q = t/u$, then $p, q \in R$ and we have $1 = ap + bq$. This implies that

$$c = (ap + bq)c = apc + qbc.$$

By assumption there is $v \in R$ with $bc = va$. Thus

$$c = apc + qav = a(pc + qv).$$

Thus $a \mid c$ and we obtain our claim.

2. Show that every principal ideal domain is a unique factorization domain.

Solution: Let $r \in R \backslash (R^* \cup \{0\})$. We want to show that there exist irreducible elements $r_1, \ldots, r_n$ such that $r = r_1 \cdots r_n$.

If r is irreducible, we are done.

So assume r is not irreducible. Then $r = r_1 r_2$ where neither r_1 nor r_2 are units. If r_1 and r_2 are irreducible, then the proof is complete.

If r_1 is not irreducible, then $r_1 = r_{11} r_{12}$, where neither r_{11} nor r_{12} are units. Continuing this way, we get a proper inclusion of ideals

$$(r) \subset (r_1) \subset (r_{11}) \subset \cdots \subset R.$$

If this process finishes in a finite number of steps, the proof is complete. But, we know by Exercise **1**.a that this is the case.

3. Consider the ring $R := \mathbb{Z}[i] \subset \mathbb{C}$ with the so called *field norm*

$$N\colon R \to \mathbb{Z}_{\geqslant 0},\ a+bi \mapsto (a+bi)(a-bi) = a^2+b^2.$$

(a) Prove that R is a Euclidean ring with respect to N.

(b) Determine $\gcd(3-i, 3+i)$ and $\gcd(2-i, 2+i)$ in R.

(c) Write $3+i$ as a product of prime elements from R.

(d) Prove that each prime element of R divides exactly one prime number $p \in \mathbb{Z}$.

(e) Prove that each prime number $p \equiv 3 \pmod 4$ is a prime element of R.

Solution: (a) Let $x, y \in R$ with $y \neq 0$. We can write $\frac{x}{y} = a + bi$ with $a, b \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that

$$|a-m| \leqslant \frac{1}{2} \quad \text{and} \quad |b-n| \leqslant \frac{1}{2}$$

and let $q := m + ni$ and $r := x - yq$. From our construction we obtain:

$$\left|\frac{x}{y} - q\right|^2 = (a-m)^2 + (b-n)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

Then we have $x = yq + r$ with

$$N(r) = |x-yq|^2 = N(y)\left|\frac{x}{y} - q\right|^2 < N(y).$$

Thus R is a Euclidean ring for the function N.

(b) We will use the Euclidean algorithm with the function N:

$$\begin{aligned} 3-i &= (3+i)\cdot(1-i) + (-1+i) \quad \text{with} \quad N(-1+i) < N(3+i) \\ 3+i &= (-1+i)\cdot(-1-2i) + 0. \end{aligned}$$

This implies that

$$\gcd(3-i, 3+i) \sim \gcd(3+i, -1+i) \sim \gcd(-1+i, 0) \sim -1+i.$$

Similarly, we compute

$$2-1 = (2+i)\cdot(1-i) - 1 \quad \text{with} \quad N(-1) < N(2+i).$$

Thus $\gcd(2-i, 2+i) \sim \gcd(2+i, -1) \sim 1$.

(c) The field norm N satisfies $N(1) = 1$ and is multiplicative: for all $a, b \in R$ we have

$$N(ab) = N(a)N(b).$$

If $s \in R^\times$ is a unit, then also $s^{-1} \in R^\times$. Hence

$$N(s)\cdot N(s^{-1}) = N(ss^{-1}) = N(1) = 1.$$

On the other hand, are $\pm 1, \pm i$ the only elements $s \in R$ with $N(s) = 1$. Hence

$$s \in R^\times \iff N(s) = 1 \iff s \in \{\pm 1, \pm i\}.$$

Since $N(3+i) = 10$, we can write $3+i$ as a product of at most two elements $s, r \in R\backslash R^\times$ of norm 2 and 5. Since N is multiplicative, we have that r and s have to be irreducible. By trying out, we find that the element $N(\pm 1 \pm i) = 2$ and $N(1+2i) = 5$, and that there is a decomposition

$$3+i = (i-1)(1+2i).$$

The ring R is Euclidean, so it is also factorial, which means that irreducible elements are prime and the decomposition above is a product of prime elements.

(d) Let $a \in R$ be prime. Since a is not a unit, we have $N(a) > 1$, so that $N(a)$ has a non-trivial decomposition into prime numbers $N(a) = p_1 \cdots p_k$. Note that $N(a) = a \cdot \overline{a}$, so that a divides at least one prime number p_i, since a is prime.

Let us assume that a divides two different prime numbers p and q. Then we have that 1 is a $\mathbb{Z}$-linear combination of p and q and hence also a R-linear combination. Hence a divides the elements $1 \in R$, which is a contradiction.

(e) Let p be prime number such that $p \equiv 3 \pmod 4$. Then we have that $N(p) = p^2 \geqslant 1$ and thus $p \notin R^\times \cup \{0\}$. Let us assume that p is not a prime element of R.

Note that $N(p) = p^2$. Since R is a factorial ring and N is multiplicative, we can decompose $p = xy$ with $N(x) = N(y) = p$. Write $x = a + bi$, so that $a^2 + b^2 = p$. Note that each square number in $\mathbb{Z}$ has to be congruent to 0 or 1 modulo (4). This implies that $a^2 + b^2$ has to be congruent to $0, 1$ or 2 modulo (4). But, we assumed that $p \equiv 3 \pmod 4$, which leads to a contradiction. Hence p is a prime element in R.

4. (a) Let R be a ring with unique factorization. Prove: if $a, b, c \in R$ are nonzero, $ab = c^n$ and a and b are relatively prime then there are units $u, v \in R$ as well as elements $a', b' \in R$, such that $a = ua'^n$ and $b = vb'^n$.

(b) There are counterexamples to the conclusion of (a) if we drop the the hypothesis that R has unique factorization. Use $R = \mathbb{Z}[\sqrt{-26}]$ to give such a counterexample.

Solution: (a) Since R is a ring with unique factorization, there exist irreducible elements $a_1, \ldots, a_i, b_1, \ldots, b_j$, and $c_1 \ldots, c_k \in R$ and u, v and u_c units in R^*, for $i, j, k \in \mathbb{Z}_{\geqslant 0}$ such that there exists a unique factorisation

$$u \cdot a_1 \cdots a_i \cdot v \cdot b_1 \cdots b_j = u_c \cdot {c_1}^n \cdots {c_k}^n,$$

with $a = u \cdot a_1 \cdots a_i$, $b = v \cdot b_1 \cdots b_j$ and $c = u_c \cdot {c_1}^n \cdots {c_k}^n$.

From $a_1 \mid u_c \cdot {c_1}^n \cdots {c_k}^n$, we have that there exists an irreducible element c_l such that $a_1 = c_l$. W.l.o.g. we can assume $l = 1$, so that $a_1 = c_1$. Since a and b are relatively prime, we have that ${c_1}^n$ divides a, but not b. Continuing this process inductively, we can write

$$a_1 \cdots a_i = {c_1}^n \cdots {c_r}^n,$$

for some $r \in \mathbb{Z}_{\geqslant 0}$. Similarly, we can write

$$b_1 \cdots b_j = {c_{r+1}}^n \cdots {c_k}^n.$$

Setting $a' := c_1 \cdots c_r$ and $b' := c_{r+1} \cdots c_k$ we obtain our claim.

(b) First, note that the only units in $\mathbb{Z}[\sqrt{-26}]$ are ± 1. Let $a = 1+\sqrt{-26}$, $b = 1-\sqrt{-26}$ and $c = 3$. Then $ab = c^3$. Assume that there are units $u, v \in \{\pm 1\}$ as well as elements $a', b' \in R$, such that $a = ua'^3$ and $b = vb'^3$. Since $a' \in R$, there are $x, y \in \mathbb{Z}$ such that $a' = x + y\sqrt{-26}$. But then

$$u \cdot a'^3 = u \cdot ((x^3 - 26xy^2) + (x^2y - 26y^3)\sqrt{-26}) = 1 + \sqrt{-26}.$$

Thus we have the system of equations

$$\begin{aligned} u \cdot x(x^2 - 26y^2) &= 1 \\ u \cdot y(x^2 - 26y^2) &= 1, \end{aligned}$$

from which we obtain $x = y$. But then $u \cdot (-25)x^3 = 1$, which is not solvable in $\mathbb{Z}$.