Chapter 4

Exercises on Ring Theory

Exercises marked by (*) are considered difficult.

4.1 Rings, ideals and homomorphisms

Exercise 37. Let R be a ring and $x \in R$. Suppose there exists a positive integer n such that $x^n = 0$. Show that $1 + x$ is a unit, and so is $1 - x$.

Answer. The element $1 - x$ is a unit since

$$(1 - x)(1 + x + \ldots + x^{n-1}) = 1.$$

The element $1 + x$ is a unit since

$$(1 + x)(1 - x + x^2 - x^3 \ldots \pm x^{n-1}) = 1.$$

Exercise 38. Let R be a commutative ring, and I be an ideal of R. Show that

$$\sqrt{I} := \{x \in R \mid \text{ there exists } m \in \mathbb{N}^* \text{ such that } x^m \in I\}$$

is an ideal of R. **Answer.**

- Clearly, $0 \in \sqrt{I}$. If $a \in \sqrt{I}$, then $a^m \in I$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m \in I$, so $-a \in \sqrt{I}$. Now let $a, b \in \sqrt{I}$, so $a^n \in I$ for some $n \geq 1$ and $b^m \in I$ for some $m \geq 1$. Now let us show that $(a + b)^{n+m} \in I$. We have $(a + b)^{n+m} = \sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n + m - j \geq m$, so $b^{n+m-j} \in I$ in this case (since $b^m \in I \Rightarrow b^i \in I$ for $i \geq m$). If $n + 1 \leq j \leq n + m$, we have $j \geq n + 1$, so $a^j \in I$ in this case (since $a^n \in I \Rightarrow a^i \in I$ for $i \geq n$). Therefore all the terms in the previous sum are in I and thus $(a + b)^{n+m} \in I$. Hence $a + b \in \sqrt{I}$. We just proved that $\sqrt{I}$ is an additive subgroup of R.

- Now we have to check the second property. Let $a \in \sqrt{I}$, and $r \in R$. We have $a^n \in I$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n \in I$ and therefore $ar \in \sqrt{I}$. Therefore $\sqrt{I}$ is an ideal of R.

Exercise 39. (*) Determine all rings of cardinality p and characteristic p.

Answer. Let R be a ring of characteristic p. Consider the ring homomorphism: $\varphi : \mathbb{Z} \to R$, the characteristic of R is the natural number p such that $p\mathbb{Z}$ is the kernel of φ. We can now factorize φ in an injective map $\mathbb{Z}/p\mathbb{Z} \to R$. If now we further assume that R has cardinality p, we have that $\mathbb{Z}/p\mathbb{Z}$ and R have same cardinality, and thus we have an isomorphism. This means that the only ring of cardinality and characteristic p is $\mathbb{Z}/p\mathbb{Z}$.

Exercise 40. Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Prove that $Nil(R)$ is an ideal of R.

2. Show that if $r \in Nil(R)$, then $1 - r$ is invertible in R.

3. Show, with a counter-example, that $Nil(R)$ is not necessarily an ideal anymore if R is not commutative.

1.
   - Clearly, $0 \in Nil(R)$. If $a \in Nil(R)$, then $a^m = 0$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m = 0$, so $-a \in Nil(R)$. Now let $a, b \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$ and $b^m = 0$ for some $m \geq 1$. Now let us show that $(a+b)^{n+m} = 0$. We have $(a+b)^{n+m} = \sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n+m-j \geq m$, so $b^{n+m-j} = 0$ in this case (since $b^m = 0 \Rightarrow b^i = 0$ for $i \geq m$). If $n+1 \leq j \leq n+m$, we have $j \geq n+1$, so $a^j = 0$ in this case (since $a^n = 0 \Rightarrow a^i = 0$ for $i \geq n$). Therefore all the terms in the previous sum are 0 and thus $(a+b)^{n+m} = 0$. Hence $a + b \in Nil(R)$. We just proved that $Nil(R)$ is an additive subgroup of R.
   - Now we have to check the second property. Let $a \in Nil(R)$, and $r \in R$. We have $a^n = 0$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n = 0$ and therefore $ar \in Nil(R)$. Therefore $Nil(R)$ is an ideal of R.

2. If $r \in Nil(R)$, then $r^m = 0$ for some $m \geq 1$. Then $1 + r + r^2 + \cdots + r^{m-1}$ is the inverse of $1 - r$ since

$$(1-r)(1+r+r^2+\cdots+r^{m-1}) = 1+r+r^2+\cdots+r^{m-1}-r-r^2+\cdots+r^m = 1-r^m = 1.$$

3. If $R = M_2(\mathbb{C})$, let $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $a^2 = b^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so $a, b \in Nil(R)$, but $a + b$ does not lie in $Nil(R)$, since $(a + b)^2 = I_2$, and $I_2^n = I_2$ for all $n \geq 1$.

Exercise 41. Determine whether the following maps are ring homomorphisms:

1. $f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_1(x) = x + 1$.
2. $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_2(x) = x^2$.
3. $f_3 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_3(x) = 4x$.
4. $f_4 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_4(x) = 6x$.

Answer.

1. Since $f_1(0) = 1$, f_1, f cannot be a ring homomorphism.
2. Since $f_2(x + y) = x^2 + y^2 + 2xy \neq x^2 + y^2 = f_2(x) + f_2(y)$, f_2 cannot be a ring homomorphism.
3. Since $f_3(xy) = 4xy \neq xy = f_3(x)f_3(y)$, f_3 cannot be a ring homomorphism.
4. Since $f_4(1) \neq 1$, f_4 cannot be a ring homomorphism!

Exercise 42. Consider the ring $\mathcal{M}_n(\mathbb{R})$ of real $n \times n$ matrices. Are the trace and the determinant ring homomorphisms?

Answer. The trace is not multiplicative, since

$$2 = \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \cdot \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 4.$$

The determinant is not additive:

$$4 = \det\left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\right) \neq \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 2.$$

Thus none of them are ring homomorphisms.

4.2 Quotient rings

Exercise 43. Compute the characteristic of the following rings R:

1. $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$,
2. $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$,

3. $R = \mathbb{Z}[j]/(2-5j)$, where j denotes a primitive 3rd root of unity ($j^3 = 1$ but $j^2 \neq 1$).

Answer. In this exercise, we use the notation $\overline{x}$ to denote an element in the quotient group involved.

1. For $1 \leq m \leq n-1$, we have $m \cdot \overline{1} = \overline{m} \neq 0$, since m is not a multiple of n. But $n \cdot \overline{1} = \overline{n} = \overline{0}$. So $\mathrm{char}(R) = n$ by definition of the characteristic.

2. If $m \in \mathbb{Z}$, we will denote by respectively by $\overline{m}, [m], \tilde{m}$ its class modulo $2, 4$ and 10. Assume that $m(\overline{1}, [1], \tilde{1}) = (\overline{0}, [0], \tilde{0})$. Then we have
$$(\overline{m}, [m], \tilde{m}) = (\overline{0}, [0], \tilde{0}),$$
which implies that m is a multiple of $2, 4$ and 10. Hence m is a multiple of the lowest common multiple of $2, 4$ and 10, which is 20. Conversely, $20(\overline{1}, [1], \tilde{1}) = (\overline{20}, [20], \tilde{20}) = (\overline{0}, [0], \tilde{0})$. Therefore $\mathrm{char}(R) = 20$.

3. Here we have $(2-5j)(2-5j^2) = 4 - 10(j+j^2) + 25j^3 = 4 + 10 + 25 = 39$. Hence $39 \cdot \overline{1} = \overline{39} = \overline{(2-5j) \cdot (2-5j^2)} = \overline{0}$. Then the characteristic of R is finite and divides 39. Therefore the characteristic of R is $1, 3, 13$ or 39. Now let $c = \mathrm{char}(R) > 0$. Since $c \cdot 1_R$ lies in the ideal $(2-5j)$, then $c = (2-5j)(a+bj)$ for some $a, b, \in \mathbb{Z}$. Hence $|c|^2 = |2-5j|^2|a+bj|^2$, so
$$c^2 = 39(a^2 + b^2 - ab)$$
and therefore $39|c^2$. The only value (among $1, 3, 13$ and 39) for which it is possible is $c = 39$. Thus $\mathrm{char}(R) = 39$.

Exercise 44. Prove the following isomorphisms:

1. $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$.

2. $\mathbb{Z}[X]/(n, X) \simeq \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$.

3. $\mathbb{Z}[X]/(n) \simeq (\mathbb{Z}/n\mathbb{Z})[X]$, $n \geq 2$.

Answer.

1. Consider $\varphi : m \in \mathbb{Z} \mapsto m \cdot 1_R = \overline{m} \in \mathbb{Z}[i]/(1+i)$. This is a ring homomorphism. It is surjective. Indeed, let $\overline{a+bi} \in \mathbb{Z}[i]/(1+i)$. We have $\overline{a+bi} = \overline{(b-a) + a(1+i)} = \overline{b-a}$, so $\overline{a+bi} = \varphi(b-a)$. Now $\ker(\varphi) = c \cdot \mathbb{Z}$, where $c = \mathrm{char}(R)$ by definition of the characteristic. By direct computation, we get $\mathrm{char}(R) = 2$ (since R is not the trivial ring and $(1+i)(1-i) = 2$). Therefore $\ker(\varphi) = 2\,\mathbb{Z}$. Now use the first isomorphism theorem.

2. Let us consider $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P(0)} \in \mathbb{Z}/n\,\mathbb{Z}$. This is the composition of the ring homomorphisms $P \in \mathbb{Z}[X] \mapsto P(0) \in \mathbb{Z}$ and $m \in \mathbb{Z} \mapsto \overline{m} \in \mathbb{Z}/n\,\mathbb{Z}$, so it is a ring homomorphism. It is surjective: for $\overline{m} \in \mathbb{Z}/n\,\mathbb{Z}$, we

have $\varphi(m) = \overline{m}$, where $m \in \mathbb{Z} \subset \mathbb{Z}[X]$ is considered as a constant polynomial. Now we have $\ker(\varphi) = \{P \in \mathbb{Z}[X] | P(0) \text{ is divisible by } n\}$, which equals (n, X). Hence $\ker(\varphi) = (n, X)$; now applying the first isomorphism theorem, we get the result.

3. Consider the reduction modulo n, $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P} \in (\mathbb{Z}/n\mathbb{Z})[X]$. We have that φ is a ring homomorphism. It is surjective: let $f \in (\mathbb{Z}/n\mathbb{Z})[X]$, $f = \overline{a}_0 + \cdots + \overline{a}_m X^m, a_i \in \mathbb{Z}$. Then let $P = a_0 + \cdots + a_m X^m \in \mathbb{Z}[X]$. By definition of $\overline{P}$, we have $\varphi(P) = f$. Now let us compute the kernel of φ. Let $P = a_0 + \cdots + a_m X^m$. We have $\varphi(P) = 0 \iff \overline{a}_0 + \cdots + \overline{a}_m X^m = 0$. This is equivalent to say that $\overline{a}_i = \overline{0}$ for all i, which means that $n | a_i$ for all i. This is equivalent to say that $P = n \cdot Q$, for some $Q \in \mathbb{Z}[X]$. Hence $\ker(\varphi) = (n)$. Now apply the first isomorphism theorem.

4.3 Maximal and prime ideals

Exercise 45. Show that a non-zero principal ideal is prime if and only if it is generated by a prime element.

Answer. If p is prime then consider the principal ideal $pR = \{pr,\ r \in R\}$. To show that pR is prime, we have to show that if $ab \in pR$ then either a or b is in pR. If $ab \in pR$, then $ab = pr$ for some $r \in R$. Since p is prime, it has to divide either a or b, that is either $a = pa'$ or $b = pb'$. Conversely, take a principal ideal cR which is prime, thus if $ab \in cR$, either $a \in cR$, that is $a = ca'$, or $b \in cR$, that is $b = cb'$. We have thus shown that if $c | ab$, then $c | a$ or $c | b$.

Exercise 46. Are the ideals $(X, X+1)$, $(5, X^2+4)$ and $(X^2+1, X+2)$ prime/maximal in $\mathbb{Z}[X]$?

Answer.

- $I = (X, X+1) = \mathbb{Z}$ since $1 = (X+1) - X$, thus I is not a proper ideal and cannot be prime.
- Consider $\mathbb{Z}[X]/(5, X^2+4) \simeq \mathbb{Z}_5[X]/(X^2+4)$, and $(X^2+4) = (X-\bar{1})(X+\bar{1})$ is reducible modulo 5, thus this quotient is not an integral domain and thus the ideal is not prime.
- $I = (X^2+1, X+2) = (X+2, 5)$ since $(X+2)^2 - 4(X+2) + 5 = X^2 + 1$, then $\mathbb{Z}[X]/I \simeq \mathbb{Z}_5[X]/(X+\bar{2})$ where $X+\bar{2}$ is irreducible in $\mathbb{Z}_5[X]$ thus the quotient is a field and I is maximal.

Exercise 47. 1. Consider the ring $R = \mathbb{Z}[i]$ and the ideal $I = (1+i)$ in R. Is I prime? Is I maximal?

2. Consider the ring $R = \mathbb{Z}[j]$ and the ideal $I = (2 - rj)$ in R. Is I prime? Is I maximal? (j is a primitive 3rd root of unity.)

3. Consider the ring $R = \mathbb{Z}[X]$ and the ideal $I = (n)$ in R. Is I prime? Is I maximal?

Answer.

1. We have $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$, which is a field, so $(1+i)$ is maximal (hence prime).

2. The characteristic of $\mathbb{Z}[j]/(2-5j)$ is 39 which is not a prime number (see Exercise 43), so $\mathbb{Z}[j]/(2-5j)$ is not an integral domain. Hence $(2-5j)$ is not prime and therefore not maximal.

3. We have $\mathbb{Z}[X]/(n) \simeq \mathbb{Z}/n\mathbb{Z}[X]$. We have that $\mathbb{Z}/n\mathbb{Z}[X]$ is an integral domain if and only if $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. Hence (n) is a prime ideal if and only if n is a prime number. It is never maximal since $\mathbb{Z}/n\mathbb{Z}[X]$ is not a field for any n (X has no inverse).

Exercise 48. Consider the ring $R = K[X]$ and the ideal of R given by $I = (X-a)$, where K is a field, and $a \in K$. Is I maximal? Is I prime?

Answer. Let $\varphi : P \in K[X] \mapsto P(a) \in K$. This is a ring homomorphism, which is surjective: indeed, if $\lambda \in K$, then $\varphi(\lambda) = \lambda$, where $\lambda \in K \subset K[X]$ is viewed as a constant polynomial. We now determine the kernel of φ. Let $P \in K[X]$. We can write $P = Q(X).(X-a) + c$, for some $Q \in K[X]$ and $c \in K$. (Indeed, it suffices to proceed to the division of P by $X - a$. The remainder is either zero or has degree < 1, that is degree 0, which means that the remainder is a constant.) Then we have $P(a) = Q(a).(a-a)+c = c$. Therefore, $\varphi(P) = 0 \iff c = 0 \iff P$ is a multiple of $X - a$. Hence $\ker(\varphi) = (X-a)$ (the principal ideal generated by $X - a$). Using the first isomorphism theorem, we get that $K[X]/(X-a) \simeq K$. Since $K[X]/(X-a) \simeq K$, and K is a field, then $K[X]/(X-a)$ is a field as well and $(X-a)$ is maximal (hence prime).

Exercise 49. (*) Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Show that $Nil(R)$ is contained in the intersection of all prime ideals of R.

2. Show that $Nil(R/Nil(R)) = 0$.

Answer.

1. Let $a \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$. Assume that there is a prime ideal $\mathfrak{p}$ for which $a \notin \mathfrak{p}$. We have $a^n = 0 \in \mathfrak{p}$. Since $a^n = a^{n-1}.a$ and $\mathfrak{p}$ is a prime ideal, then $a^{n-1} \in \mathfrak{p}$ or $a \in \mathfrak{p}$. By assumption on a, we have $a \notin \mathfrak{p}$, so necessarily $a^{n-1} \in \mathfrak{p}$. But $a^{n-1} = a^{n-2}.a \in \mathfrak{p}$, so $a^{n-2} \in \mathfrak{p}$ for the same reasons, and by induction we get $a \in \mathfrak{p}$, a contradiction. Therefore a lies in all the prime ideals of R.

2. Let $\overline{a} \in Nil((R/Nil(R)))$, so $\overline{a}^n = \overline{0}$ for some $n \geq 1$. Then $\overline{a^n} = \overline{0}$, which means that $a^n \in Nil(R)$ by definition of the quotient ring. Therefore, there exists $m \geq 1$ such that $(a^n)^m = 0$, so $a^{nm} = 0$, which means that $a \in Nil(R)$. Hence $\overline{a} = \overline{0}$.

Exercise 50. Let $R = \mathbb{Z}[X]$, and let $n \geq 1$.

- Show that the ideal (n, X) is given by

$$(n, X) = \{p(X) \in \mathbb{Z}[X],\ p(0) \text{ is a multiple of } n\}.$$

- Show that (n, X) is a prime ideal if and only if n is a prime number.

Answer.

- Let $P \in (n, X)$, so $P = n.Q_1 + X.Q_2$ for some $Q_1, Q_2 \in \mathbb{Z}[X]$. Then $P(0) = n.Q_1(0) \in n\mathbb{Z}$ (we have $Q_1(0) \in \mathbb{Z}$ since $Q_1 \in \mathbb{Z}[X]$), that is $P(0)$ is a multiple of n. Conversely, assume that $P \in \mathbb{Z}[X]$ is such that $P(0)$ is a multiple of n, and write $P = a_n X^n + \cdots + a_1 X + a_0$. Then $P(0) = a_0$, so by assumption $a_0 = n.m$ for some $m \in \mathbb{Z}$. Now we get $P = n.m + X.(a_n X^{n-1} + \cdots + a_2 X + a_1)$, so $P \in (n, X)$.

- If n is not a prime number, then we can write $n = n_1.n_2, 1 < n_1, n_2 < n$. Now consider $P_1 = n_1, P_2 = n_2 \in \mathbb{Z}[X]$ (constant polynomials). We have $P_1.P_2 = n_1.n_2 = n \in (n, X)$, but P_1 and P_2 are not elements of (n, X). Indeed, $P_1(0) = n_1$ and $P_2(0) = n_2$, but n_1, n_2 are not multiples of n by definition. Hence (n, X) is not a prime ideal. Now assume that n is equal to a prime number p. First of all, $(p, X) \neq \mathbb{Z}[X]$, because $1 \notin (p, X)$ for example. Now let $P_1, P_2 \in \mathbb{Z}[X]$ such that $P_1.P_2 \in (p, X)$. Then $(P_1.P_2)(0)$ is a multiple of p by the previous point, that is $p|P_1(0).P_2(0)$. Since p is a prime number, it means that $p|P_1(0)$ or $p|P_2(0)$, that is $P_1 \in (p, X)$ or $P_2 \in (p, X)$. Hence (p, X) is a prime ideal.

4.4 Polynomial rings

Exercise 51. Set

$$E = \{p(X) \in \mathbb{Z}[X] \mid p(0) \text{ is even }\},\ F = \{q(X) \in \mathbb{Z}[X] \mid q(0) \equiv 0 (\text{mod } 3)\}.$$

Check that E and F are ideals of $\mathbb{Z}[X]$ and compute the ideal $E + F$. Furthermore, check that $E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] | p(0) \equiv 0 \ (\text{mod } 6)\ \}$.

Answer. If $p(X) = \sum_{k=0}^{n} p_k X^k$, then

$$E = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z}\} \quad \text{and} \quad F = \{q(X) \in \mathbb{Z}[X] \mid q_0 \in 3\mathbb{Z}\}.$$

Thus E and F are ideals of $\mathbb{Z}[X]$ since $2\mathbb{Z}$ and $3\mathbb{Z}$ are ideals of $\mathbb{Z}$. If $\sum_k c_k X^k = \left(\sum_k p_k X^k\right) \cdot \left(\sum_k q_k X^k\right)$, then $c_0 = p_0 q_0$ and thus

$$E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z} \cdot 3\mathbb{Z}\} = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 6\mathbb{Z}\}.$$

Similarly,

$$E + F = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z} + 3\mathbb{Z}\} \underbrace{=}_{\text{Bezout}} \{p(X) \in \mathbb{Z}[X] \mid p_0 \in \mathbb{Z}\} = \mathbb{Z}[X].$$

Exercise 52. Show that if F is a field, the units in $F[X]$ are exactly the nonzero elements of F.

Answer. Let $f(X) \in F[X]$ of degree n, $f(X)$ is a unit if and only if there exists another polynomial $g(X) \in F[X]$ of degree m such that $f(X)g(X) = 1$. Because F is a field (thus in particular an integral domain), $f(X)g(X)$ is a polynomial of degree $n+m$, thus for the equality to hold, since 1 is a polynomial of degree 0, we need $n+m = 0$, thus both f and g are constant, satisfying $fg = 1$, that is they are units of F, that is nonzero elements since F is a field.

Exercise 53. There exists a polynomial of degree 2 over $\mathbb{Z}/4\mathbb{Z}$ which has 4 roots. True or false? Justify your answer.

Answer. Take the polynomial $2X(X-1)$.

Exercise 54. Let R be a ring, and let $a \neq 0 \in R$ such that there exists an integer n with $a^n = 0$. Show that $R^* \subset (R[X])^*$ and $R^* \neq R[X]^*$, where R^* and $R[X]^*$ denote respectively the group of units of R and $R[X]$.

Answer. Clearly $R^* \subseteq R[X]^*$. We need to show that the inclusion is strict, that this, there exists an element in $R[X]^*$ which is not in R^*. Take $f(X) = 1 - aX$. We have

$$(1 - aX)(1 + aX + (aX)^2 + \ldots + (aX)^{n-1}) = 1,$$

and f does not belong to R^*.

4.5 Unique factorization and Euclidean division

Exercise 55.

Show that the ideal generated by 2 and X in the ring of polynomials $\mathbb{Z}[X]$ is not principal.

Answer. We have that

$$\langle 2, X\rangle = \{2r(X) + Xs(X),\ r(X), s(X) \in \mathbb{Z}[X]\},$$

and assume there exists $f(X) \in \mathbb{Z}[X]$ such that $\langle 2, X\rangle = (f(X))$. Since $2 \in (f(X))$, then $f(X) = \pm 2$. Since $X \in (f(X))$, we should have $X = \pm 2g(X)$, a contradiction.

Exercise 56. Show that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain. (Hint: use the same technique as the one seen for $\mathbb{Z}[\sqrt{2}]$.)

Answer. Consider the ring

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3},\ a, b \in \mathbb{Z}\}$$

with

$$\Psi(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

Take $\alpha, \beta \neq 0$ in $\mathbb{Z}[\sqrt{3}]$, and compute the division in $\mathbb{Q}(\sqrt{3})$:

$$\alpha/\beta = q',$$

with $q' = x + \sqrt{3}y$ with x, y rational. Let us now approximate x, y by integers x_0, y_0, namely take x_0, y_0 such that

$$|x - x_0| \leq 1/2,\ |y - y_0| \leq 1/2.$$

Take

$$q = x_0 + y_0\sqrt{3},\ r = \beta((x - x_0) + (y - y_0)\sqrt{3}),$$

where clearly $q \in \mathbb{Z}[\sqrt{3}]$, then

$$\begin{aligned} \beta q + r &= \beta(x_0 + y_0\sqrt{3}) + \beta((x - x_0) + (y - y_0)\sqrt{3}) \\ &= \beta(x + y\sqrt{3}) = \beta q' = \alpha, \end{aligned}$$

which at the same time shows that $r \in \mathbb{Z}[\sqrt{3}]$. So far this is exactly what we did in the lecture. We are also left to show that $\Psi(r) < \Psi(\beta)$. We have

$$\begin{aligned} \Psi(r) &= \Psi(\beta)\Psi((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| \\ &\leq \Psi(\beta)[|x - x_0|^2 + |d||y - y_0|^2] \\ &\leq \Psi(\beta)\left(\frac{1}{4} + |3|\frac{1}{4}\right) \end{aligned}$$

though here we notice that we get $\frac{1}{4} + |3|\frac{1}{4} = 1$. So this is not good enough! But let us see what this means to get 1: this happens only if $|x - x_0|^2 = |y - y_0|^2 = 1/4$, otherwise we do get something smaller than 1. Now if $|x - x_0|^2 = |y - y_0|^2 = 1/4$, we have from the second equation that

$$\Psi = \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| = \Psi(\beta)|\frac{1}{4} - \frac{3}{4}| < 1$$

and we are done.

Exercise 57. True/False.

Q1. Let R be a ring, and let r be an element of R. If r is not a zero divisor of R, then r is a unit.

Q2. A principal ideal domain is a euclidean domain.

Q3. Hamilton's quaternions form a skew field.

Q4. The quotient ring $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is a field.

Q5. A field is a unique factorization domain.

Q6. The ideal $(5,i)$ in $\mathbb{Z}[i]$ is principal.

Q7. Let R be a ring, and M be a maximal ideal, then R/M is an integral domain.

Answer.

Q1. This cannot be true in general! Take $\mathbb{Z}$ for example. It has no zero divisor, but apart 1 and -1, no other element is a unit! Actually, in an integral domain, there is no zero divisor, which does not mean it is an field.

Q2. A euclidean domain is a principal ideal domain. The converse is not true. Take for example $\mathbb{Z}[(1+i\sqrt{19})/2]$. It is a principal ideal domain, but it is not a euclidean domain.

Q3. A skew field is non-commutative field. Hamilton's quaternions are non-commutative, and we have seen that every non-zero quaternion is invertible (the inverse of q is its conjugate divided by its norm).

Q4. It is actually a field. You can actually compute the quotient ring explicitly, this shows that $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is isomorphic to the field of 2 elements $\{0,1\}$.This can be done using the first isomorphism for rings.

Q5. It is true since every non-zero element is a unit by definition.

Q6. It is true! With no computation, we know it from the theory: We know that $\mathbb{Z}[i]$ is a euclidean domain, and thus it is a principal domain, so all ideals including this one are principal.

Q7. Who said the ring R is commutative? The statement seen in the class is about commutative rings. It is not true for non-commutative rings. Here is an example: take $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ (ring of quaternions with integer coefficients), pR is a maximal ideal of R (p odd prime) but R/pR is actually isomorphic to $M_2(\mathbb{Z}/p\mathbb{Z})$ and thus is not an integral domain.