Exercise 1. Consider the ring $\mathbb{Z}_n$, with $n \geq 2$.

- $\mathbb{Z}_n^* = \{[x] \in \mathbb{Z}_n : (x,n) = 1\}$ [1]. In fact $(x,n) = 1 \iff \exists a,b \in \mathbb{Z}\big(ax + bn = 1\big) \iff \exists a,b \in \mathbb{Z}\big([ax+bn] = [1]\big) \iff \exists a,b \in \mathbb{Z}\big([ax] + [bn] = [1]\big) \iff \exists a,b \in \mathbb{Z}\big([a][x] + [b][n] = [1]\big) \iff \exists [a] \in \mathbb{Z}_n\big([a][x] = 1\big)$.
- $\mathrm{Zdv}(\mathbb{Z}_n) = (\mathbb{Z}_n^*)^C$. It is sufficient to show $\supseteq$. If $(x,n) = d \neq 1$ then $x\frac{n}{d} = \frac{x}{d}n = cn$ for some $c \in \mathbb{Z}$, i.e. $[x][\frac{n}{d}] = [0]$, and since $d \neq 1 \Rightarrow \frac{n}{d} < n \Rightarrow [\frac{n}{d}] \neq 0$ we are done.

Exercise 2. Let R be an euclidean domain and $f : R\setminus\{0\} \to \mathbb{N}$ a norm on R. Let $I \lhd R$ an ideal. It is sufficient to show $I \subseteq gR$ for some g. Let $g \in I\setminus\{0\}$ be such that $f(g) = \min f[I]$. Let $a \in I$. By hypothesis we have $a = gq + r$ for some $q,r \in R$ such that either $r = 0$ or $f(r) < f(g)$. But then $r = a - gq \in I$, thus $r = 0$ necessarily by minimality. Therefore $a = gq$, and we are done.

Exercise 3. Let I be an ideal of a ring R. Let $\mathbb{L}_I$ be the set of all ideals of R which contain I. Let $(\mathbb{L}\left(R/I\right), \subseteq)$ be the set of all ideals of R/I. Let the mapping $\Phi_I : (\mathbb{L}_I, \subseteq) \to (\mathbb{L}\left(R/I\right), \subseteq)$ be defined as:

$$\forall a \in \mathbb{L}_I : \Phi_I\left(a\right) = \pi\left(a\right)$$

where $q : a \to a/J$ is the canonical epimorphism from a to a/J from the definition of quotient ring. Then Φ_I is an isomorphism.

Dimostrazione. Let $b \in \mathbb{L}_I$. Of course, $I \subseteq b$. Thus $\pi^{-1}\left(\pi\left(b\right)\right) = b + J = b$. Furthermore, let c be an ideal of R/I. Then $\pi\left(\pi^{-1}\left(c\right)\right) = c$. Thus Φ_I is a bijection, and we have that $\forall c \in \mathbb{L}\left(R/I\right)\left(\pi^{-1}\left(\Phi_I\right)c = \pi^{-1}\left(c\right)\right)$.
Now to show that Φ_I is an isomorphism, let $b_1, b_2 \in \mathbb{L}_I$. If $b_1 \subseteq b_2$, then $\pi\left(b_1\right) \subseteq \pi\left(b_2\right)$.
Conversely, suppose $\pi\left(b_1\right) \subseteq \pi\left(b_2\right)$. By what we have just proved, $b_1 = \pi^{-1}\left(\pi\left(b_1\right)\right) \subseteq \pi^{-1}\left(\pi\left(b_2\right)\right) = b_2$.
Thus Φ_J is an isomorphism. $\square$

Exercise 4. Let $\mathcal{F}$ be the set of ideals of R of the form xR, with x not a unit and such that x cannot be decomposed in the form: $x = up_1 \cdots p_r$ with u a unit and $p_1, \ldots, p_r$ irreducible. We show towards a contradiction that $\mathcal{F} = \emptyset$. Suppose $\mathcal{F} \neq \emptyset$. Since R is noetherian, we can choose a maximal element $aR \in \mathcal{F}$. By construction, a is not irreducible, so we can write $a = bc$ with b, c non-units and not associates. Since a and b are not associate, we have $bR \subsetneq aR$ and $aR \subsetneq bR$ (??????????). Since

[1] It is immediate to check that the set is well-defined.

aR is assumed maximal, this means that bR and cR do not belong to $\mathcal{F}$. Therefore there exist units u, v and irreducible elements $p_1, \ldots, p_r, q_1, \ldots, q_s$ such that:

$$b = up_1 \cdots p_r \text{ and } c = vq_1 \cdots q_s$$

But this implies that

$$a = bc = (uv)\, p_1 \cdots p_r \cdot q_1 \cdots q_s$$

which is a contradiction, since we assumed that a could not be written in this form.

Exercise 5. Let R be a PID. Suppose we have an ascending chain of principal ideals $(a_1) \subseteq (a_2) \subseteq \ldots$ and let I be the union $I = \bigcup_{i=1}^{\infty}(a_i)$. Obviously I is an ideal, and is a principal ideal because it is in a PID. Therefore, it is generated by a single element, $I = (a)$. Since $a \in I$, $a \in (a_N)$ for some N. Then if $i \geq N$, then we have $(a) = (a_N)$, so it satisfies the ascending chain condition of principal ideals.

Let an element a be irreducible. If $1 \in (a)$, then a would be a unit, so (a) must be a proper ideal. If there is no maximal proper ideal containing (a), then the ascending chain condition would not be satisfied, so we can conclude that there is a maximal ideal proper ideal I containing (a) (Note: This does not require the Zorn's lemma or axiom of choice, since we did not use the theorem on maximal ideals). This ideal must be a principal ideal (b) by hypothesis, but since $a \in (b)$, we have $b|a$, and since a is irreducible, b must either be a unit or an associate of a. Since (b) is a proper ideal, b must not be a unit, so it must be an associate of a. Therefore, $(a) = (b)$, so (a) is maximal. However, all maximal ideals are clearly prime, so (a) is a prime ideal, which implies that a is prime.

Exercise 6.

- Let R be a finite integral domain. Let $a \in R$ such that $a \neq 0$. We wish to show that a has a product inverse in R. So consider the function $f : R \to R$ defined by $f : x \mapsto ax$. We first show that the kernel of f is just $\{0\}$. We have $\ker(f) = \{x \in R : f(x) = 0\} = \{x \in R : ax = 0\}$. Since R is an integral domain, it has no zero divisors (except 0) and thus $ax = 0$ means that $a = 0$ or $x = 0$. Since $a \neq 0$, then necessarily $x = 0$. Therefore, $\ker(f) = \{0\}$ and so f is injective.
  Next, by the Pigeonhole Principle, f is surjective as well. Finally, since f is surjective and $1 \in R$, we have:

  $$\exists\, x \in R : f(x) = ax = 1$$

  So x is the inverse of a and we are done.

Exercise 7. Let $R = \mathbb{Z}[\sqrt{-5}]$, $\alpha = 6$ and $\beta = 2(1+\sqrt{-5})$. Then $\gcd(\alpha, \beta) = \emptyset$.

Dimostrazione. Define a function $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ by

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Then:

- It's easy to check that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.
- Thus, if $\alpha|\beta$ in $\mathbb{Z}[\sqrt{-5}]$, then $N(\alpha)|N(\beta)$ in $\mathbb{Z}$.
- $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit if and only if $N(\alpha) = 1$. In fact, $\alpha\alpha' = 1 \Rightarrow N(\alpha)N(\alpha) = N(1) = 1 \Rightarrow N(\alpha) = N(\alpha') = 1$, and viceversa $N(\alpha) = a^2 + 5b^2 = 1 \Rightarrow b = 0 \wedge a^2 = 1 \Rightarrow \alpha = \pm 1$.
- Of course $a^2 + 5b^2 \neq 2, 3$ for all $a, b \in \mathbb{Z}$. Thus there are no elements in $\mathbb{Z}[\sqrt{-5}]$ with $N(\alpha) = 2$ or $N(\alpha) = 3$.
- It follows that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible. In fact $N(2) = 4, N(3) = 9$ and $N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6$. Suppose $2 = ab$, which implies $N(a)N(b) = 4$. Since the last point, this means necessarily that $N(a) = 1$ or $N(b) = 1$, and by the third point this means that a or b is a unit, i.e. 2 is irreducible.
  For the other elements it's sufficient to adapt the same argument.

Now suppose that $\gcd(\alpha, \beta) = \delta$ for some $\delta \in \mathbb{Z}[\sqrt{-5}]$. Since $\beta = 2(1+\sqrt{-5})$ and $\alpha = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, this means that $2|\delta$ and $(1+\sqrt{-5})|\delta$, thus $2(1+\sqrt{-5})|\delta$, i.e. $\beta|\delta$. Therefore $\beta|\alpha$, i.e. $2(1+\sqrt{-5})|2\cdot 3$, thus $(1+\sqrt{-5})|3$, which is not possible since 3 is irreducible and $(1+\sqrt{-5})$ is not associate to 3 (because the only units are $+1, -1$).

$\square$

Exercise 9. Let R be a ring and let aR be the the ideal generated by a. Suppose that $a = xy$ for some $x, y \in R$. Then, clearly $xy \in (a)$. So, $x \in (a)$ or $y \in (a)$, since (a) is a prime ideal. Thus, $x = am$, or $y = an$ for some $m, n \in R$. Since we can rewrite the last assertion as $a|x$ or $a|y$, we conclude that a is prime.
Viceversa, suppose that a is prime. To show that a is a prime ideal, suppose that $xy \in (a)$ for some $x, y \in R$. Since $xy \in (a)$, we have that $xy = ac$ for some $c \in R$. We can rewrite this as $a|(xy)$. However, since a is prime, this implies that $a|x$ or $a|y$. So, $x = am$ or $y = an$ for some $m, n \in R$. Hence, $x \in (a)$ or $y \in (a)$, as required.

An introduction to module theory. Throughout, let R be a commutative ring A. Submodules, factor module, and homomorphisms.

Definizione 0.0.1. Let M be an additive abelian group. An R-modulo structure on M is a map $\sigma : R \times M \to M$, $(\lambda, x) \mapsto \lambda \cdot x$ such that for all $\lambda, \mu \in R$ and all $x, y \in M$:

-
-
-

Esempio 0.0.2.

- If $\lambda \in R$, then $\lambda 0 = \lambda(0+0) = \lambda 0 + \lambda 0$ and hence $\lambda 0 = 0$.
- If R is a field, then an R-module is an R-vector space.
- $R = \mathbb{Z}$ every abelian group is a $\mathbb{Z}$-modulo (with the usual multiplication as scalar multiplication).
- Ring multiplication: $R \times R \to R$ is an R-module structure, i.e. R is an R-module.
- Let $f : R \to S$ be a ring hom. Then S is an R-module defined by $R \times S \to S$, $(r, s) \mapsto f(r)s$. In particular, if $R \subseteq S$ is a subring, then S is an R-module by ring multiplication (e.g., $R \subseteq R[x_1, ..., x_n]$).

Definizione 0.0.3. Let M be an R-module. A subset $N \subseteq M$ is called an $(R-)$submodule of M if

- $N \subseteq M$ is a subgroup
- For all $\lambda \in R$ and all $x \in N$, $\lambda x \in N$

Then $\sigma | R \times N : R \times N \to N$ is an R-module structure on N, and N is an R-modulo.

Remarks and examples

- Let G be an abelian group and $H \subseteq G$ a subset. Then $H \subseteq GG$ is a subgroup iff $H \subseteq G$ is a $\mathbb{Z}$-submodule.
- Let $I \subseteq R$ be a subset. Then $I \subseteq R$ is an ideal iff $I \subseteq R$ is an R-submodule.
- $0 = \{0_R\}$ and M are R-submodules of M. M is called simple if $0 \neq M$, and 0 and M are the only submodules of M.

- If $(M_\lambda)_{\lambda\in\Lambda}$ is a family of R-submodules, then $\bigcap_{\lambda\in\Lambda} M_\lambda$ and $\sum_{\lambda\in\Lambda} M_\lambda = \{\sum_{\lambda\in\Lambda} m_\lambda \mid m_\lambda \in M_\lambda, m_\lambda > 0 \text{ for almost all } \lambda \in \Lambda\}$ are submodules of M. In particular, if M_1 and $M_2 \subseteq M$ are submodules, then $M_1 + M_2 = \{m_1 + m_2 \mid m_1 \in M_1, m_2 \in M_2\} \subseteq M$ is a submodule.

Definizione 0.0.4. Let M be an R-module and $R \subseteq M$ a subset. Then

$$_R < E >=< E >= \{\sum_{i=1}^{n} \lambda_i x_i \mid n \in \mathbb{N}, \lambda_1, ..., \lambda_n \in R, x_1, ..., x_n \in E\}$$

is the submodule generated by E.

Remarks 1.

- Since $< E >= \bigcap_{E \subseteq N \subseteq M, N R-\text{submodule}} N = \sum_{x\in E} Rx$, $< E >$ is the smallest submodule of M containing E.

- If $E = \{x\}$, then $< E >= Rx$.
  If $E = \{x_1, ..., x_n\}$, then $< E >= Rx_1 + ... + Rx_n$.
  If $(M_\lambda)_{\lambda\in\Lambda}$ is a family of submodules of M, then $< \cup_{\lambda\in\Lambda} M_\lambda >= \sum_{\lambda\in\Lambda} M_\lambda$.

- A subset $E \in M$ is called an ($R-$module) generating set of M if $_R < E >= M$. M is called finitely generated if M has a finite generating set.
  - R field: M is a f.g. R-module iff $\dim_R(M) < \infty$.
  - $R = \mathbb{Z}$: M f.g. $\mathbb{Z}$-module iff M is a f.g. abelian group.
  - $R[X]$ is not a f.g. R-module (immediate).

- Let M be a f.g. R-module. Then every generating set contains a finite generating set.

  Dimostrazione. Let $E \subseteq M$ be a finite generating set, and let $E' \subseteq M$ be an arbitrary generating set. Since $E \subseteq M =< E' >$, there is a finite subset $E'' \subseteq E'$ with $E \subseteq < E'' >$. This implies that $M =< E > \subseteq << E'' >>=< E'' >$, i.e. $E'' \subseteq E'$ is a finite generating set. $\square$

Definizione 0.0.5. Let M and N be R-modules. A map $f : M \to N$ is said to be (an R-module homomorphism if

- f is a group hom (i.e. $f(x + y) = f(x) + f(y)$).

- f is R-linear (i.e. $f(\lambda x) = \lambda f(x)$).
  Hom_R