7 Quotient ring.

◇ **7.1** Let I be an ideal of R. Since I is an abelian subgroup of R under addition, R/I is again the abelian group under addition. Define multiplication on R/I by $(a+I)\cdot(b+I)=ab+I$. Prove that
a) this definition is correct (i.e. if $a+I=a_1+I$, $b+I=b_1+I$, then $(a+I)\cdot(b+I)=(a_1+I)\cdot(b_1+I)$);
b) R/I is a commutative associative ring with unity. (This ring is called *the quotient ring*); c) the *canonical homomorphism* $\varphi: R\to R/I$, defined by $\varphi(x)=x+I$ is surjective;
d) $\forall\ f: R\to S$ — homomorphism $\exists\ i: R/\operatorname{Ker} f\to S$ – such an injective homomorphism that the diagram

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\varphi"] & S \\ R/\operatorname{Ker} f \arrow[ur, "i"'] & \end{tikzcd}$$

is commutative;
e) $R/\operatorname{Ker} f\cong \operatorname{Im} f$;
f) there is one-to-one correspondence between ideals of R containing I and ideals of R/I;
g) let $f: R\to S$ be such a homomorphism that $\operatorname{Ker} f\subset I$, then $\exists\ \bar f: R/I\to S$ – such a homomorphism that the diagram

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\varphi"] & S \\ R/I \arrow[ur, "\bar f"'] & \end{tikzcd}$$

is commutative.

◇ **7.2** Let R and S be some rings.
a) Prove that the sets $R\times\{0\}=\{(a,0),\quad a\in R\}$ and $\{0\}\times S=\{(0,b),\quad b\in S\}$ are ideals in $R\times S$. Are these ideals principal?
b) Prove that the quotient rings $(R\times S)/(R\times\{0\})\cong S$ and $(R\times S)/(\{0\}\times S)\cong R$.

◇ **7.3** Let I and J be two non-trivial ideals of a ring R. Consider the homomorphism $f: R\to(R/I)\times(R/J)$ defined by $f(x)=(x+I,x+J)$.
a) Prove that $\operatorname{Ker} f=I\cap J$.
b) Prove that f is surjective $\Leftrightarrow I+J=R$.
c) Prove that a ring R is a direct product of two rings $\Leftrightarrow$ R contains idempotent elements. [For an an idempotent element e take $I=(e)$ and $J=(1-e)$]
d) A ring R is called *boolean* if $\forall\ a\in R\ \ a^2=a$. Prove that a finite boolean ring is isomorphic to $\mathbb{Z}_2\times\ldots\times\mathbb{Z}_2$.

◇ **7.4** Prove that finite integral domain is a field.

◇ **7.5** a)Prove that if x is nilpotent then $1-x$ is invertible.
b) Prove that nil-radical is contained in all the maximal ideals.
c) Intersection of all maximal ideals is called the *Jacobson radical*. Prove that the Jacobson radical consists of all elements x such that $1-xy$ is invertible $\forall y\in R$.
d) Prove that nil-radical is contained in the Jacobson radical. Give an example when they do not coincide.

Def 7.1 An ideal I of a ring R is called *prime* if $\forall a,b\in R\ ab\in I$ implies that $a\in I$ or $b\in I$.

◇ **7.6** a) Prove that an ideal I of a ring R is prime $\Leftrightarrow$ R/I is an integral domain.
b) Prove that an ideal I of a ring R is maximal $\Leftrightarrow$ R/I is a field.
c) Prove that any maximal ideal is prime.
d) Prove that nil-radical is contained in each prime ideal.
e*) Prove that nil-radical is the intersection of all prime ideals.
f) Give an example of a non-prime ideal.
g) Give an example of a prime ideal which is not maximal.
h) Prove that R is integral domain $\Leftrightarrow$ $\{0\}$ is prime ideal.

◇ **7.7** Prove that: a) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$; b) $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$ $(a \in \mathbb{R})$; c) $\mathbb{C}[x]/(x-a) \cong \mathbb{C}$ $(a \in \mathbb{C})$;
d) $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$; e) $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$; f) $\mathbb{C}[x]/(x^2-1) \cong \mathbb{C} \times \mathbb{C}$;
g) $\mathbb{C}[x]/(x^2+1) \cong \mathbb{C} \times \mathbb{C}$; h) $\mathbb{Z}[x]/(x-a) \cong \mathbb{Z}$ $(a \in \mathbb{Z})$; i) $\mathbb{Z}[x]/(2) \cong \mathbb{Z}_2[x]$;
j) $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}_2$ (recall that $(2,x)$ is the ideal generated by 2 and x);

◇ **7.8** a) Prove that $\mathbb{Z}[x]/(2x) \cong A$ where A is the subring of $\mathbb{Z}_2[x] \times \mathbb{Z}$ defined by
$A = \{(P(x), m), \quad m \equiv P(0)(mod 2)\}$;
b) Prove that A has no nilpotent or idempotent elements; prove that all the maximal ideals of A are principal ideals generated by the elements $(P(x), 1)$, $(1, p)$ and $(x, 2)$, where $P(x) \neq x$ is an irreducible polynomial in $\mathbb{Z}_2[x]$ and $p \in \mathbb{Z}$ is an odd prime.

Def 7.2 Let R be an integral domain. An element $a \in R$, $a \neq 0$, $a \notin R^*$ is called *irreducible* if $a = bc$ implies $b \in R^*$ or $c \in R^*$.

◇ **7.9** a) Prove that if the ideal (a) is prime then a is irreducible.
b) Prove that in a principle domain the following three statements are equivalent:
(1) a is irreducible;
(2) the ideal (a) is prime;
(3) the ideal (a) is maximal.
c) Give an example of an integral domain R and of an irreducible element $a \in R$ such that the the ideal (a) is prime but not maximal.
d) Let $R = \{a + bi\sqrt{3}, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Prove that 2 is irreducible in R but (2) is not prime.

Def 7.3 Integral domain R is called *factorial* if any non-invertible element $a \in R$ may be represented as $a = p_1 \dots p_l$ where $p_1, \dots, p_l$ are some irreducible elements and this representation is unique up to an invertible factor. (This means that for any other such decomposition
$a = q_1 \dots q_s \quad l = s$ and after appropriate renumbering $(p_i) = (q_i)$.)

◇ **7.10** a) Prove that every principal domain is factorial.
b) Prove that in a factorial domain a is irreducible $\Leftrightarrow$ the ideal (a) is prime. Therefore irreducible elements in factorial domains may be also called primes.
c) Give an example of an integral domain which is not factorial.
d) Give an example of a factorial domain which is not a principal domain.
e*) Prove that if R is factorial then the polynomial ring $R[x]$ is also factorial.

◇ **7.11** a) Prove that $\mathbb{Z}[i] = \{a + bi, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a principal ring.
b) Which of the numbers 2, 3, 5, 7, 11, 13 are irreducible in $\mathbb{Z}[i]$?
c) Describe irreducible elements in $\mathbb{Z}[i]$.

◇ **7.12** a) Let R be an integral domain. Consider the relation $\sim$ on $R \times (R \setminus \{0\})$ defined by $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Prove that $\sim$ is an equivalence relation. The equivalence class of a pair (a,b) will be denoted by $\frac{a}{b}$ and called *fraction*. The set of all fractions will be denoted by K. Define the operations " + " and " $\cdot$ " on K by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
b) Prove that the operations " + " and " $\cdot$ " on K are defined correctly and K is a field under these operations. This field is called the *field of fractions* of the integral domain R. Prove that K contains the subring $\{\frac{a}{1}, \quad a \in R\}$ which is isomorphic to R.
c) Prove that if an integral domain R is a subring of a field L then the minimal subfield $K \subset L$, such that $R \subset K \subset L$ is isomorphic to the field of fractions of R.