1. *Let R be a ring, $I, J \lhd R$ and $S \leq R$. Prove that*
a) $I + J$ is the smallest ideal of R containing both I and J;
b) $IJ \lhd R$, and $IJ \leq I \cap J \lhd R$;
c) $I + S, IS, SI \leq R$.
(Remember that for $A, B \leq R$, AB is defined as $\{\sum_i a_i b_i \mid a_i \in A,\ b_i \in B\ \forall i\}$.)

Solution: It is useful to observe first that for $A, B \leq R$ both $A+B$ and AB are subgroups of $(R, +)$:
$0 = 0 + 0 \in A + B$ and $(a + b) - (a' + b') = (a - a') + (b - b') \in A + B$;
$0 = 0 \cdot 0 \in AB$, AB is defined so that it would be closed under addition, and $-\sum_i a_i b_i = \sum_i (-a_i) b_i \in AB$.
So in each part we only have to check the closedness for multiplication inside the subset (for the subset to be a subring) or by elements of R (for the subset to be an ideal).

a) For $a \in I$, $b \in J$ and $r \in R$, $(a+b)r = ar + br \in I + J$ and $r(a + b) = ra + rb \in I + J$, since $I, J \lhd R$. So $I + J \lhd R$. Clearly, $I = I + 0 \subseteq I + J$, and $J = 0 + J \subseteq I + J$, and any ideal that contains I, J must contain $I + J$, since the ideal is closed under addition. So $I + J$ is, indeed, the smallest ideal containing I and J.

b) Let $a_i \in I$, $b_i \in J$ and $r \in R$. Then $r\sum_i a_i b_i = \sum_i (ra_i) b_i \in IJ$, and $(\sum_i a_i b_i) r = \sum_i a_i (b_i r) \in IJ$, thus $IJ \lhd R$. For any i, all $a_i b_i$ are in both I and J, so $\sum_i a_i b_i$ is in both I and J, implying that $IJ \leq I \cap J$. Finally, $I \cap J$ is an ideal in R, since $0 \in I \cap J$, and for any $a, b \in I \cap J$ and for $r \in R$, $a - b$, ar and ra are in both I and J, so they are in $I \cap J$.

c) Let $a, b \in I$ and $s, t \in S$. Then $(a + s)(b + t) = ab + at + sb + st \in I + S$, since $ab, at, sb \in I$ follows from the assumption that I is an ideal. So $I + S \leq R$. The elements of $IS \cdot IS$ are sums of elements of the form $asbt$ where $a, b \in I$ and $s, t \in S$. But $I \lhd R \Rightarrow a(sb) \in I$, so $asbt \in IS$, and then $IS \cdot IS \subseteq IS$. Similarly, the summands of any element of $SI \cdot SI$ are of the form $satb$, where $a, b \in I$, $s, t \in S$, and $s(atb) \in SI$, so $SI \cdot SI \subseteq SI$. Thus both IS and SI are subrings of R.

2. *Let K be a field and $K[x, y]$ be the polynomial ring of two variables. What are the elements of the ideal I of $K[x, y]$ generated by x and y^2, that is, of the smallest ideal containing these polynomials? Determine the factor ring I by choosing an appropriate set of representatives of the cosets.*

Solution: Every polynomial, where the coefficient of 1 and y is zero, is in the generated ideal, and these, indeed, form an ideal. From this, we also get that the polynomials $a + by$ $(a, b \in K)$ form a full set of representatives of the cosets of I. The operations of the factor ring can be given, using these representatives:

$$\overline{a + by} + \overline{c + dy} = \overline{(a + c) + (b + d)y}$$
$$\overline{a + by} \cdot \overline{c + dy} = \overline{ac + (ad + bc)y},$$

because $bdy^2 \in I$, so
$(a + by + I)(c + dy + I) = ac + (ad + bc)y + bdy^2 + I = ac + (ad + bc)y + I.$

3. *Prove that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$, where $(x^2 + 1)$ is the ideal generated by $x^2 + 1$. What are the ideals of the factor ring $\mathbb{C}[x]/(x^2 + 1)$?*

Solution: The ideal I generated by x^2+1 is $\{(x^2+1)p(x) \mid p(x) \in \mathbb{R}[x]\}$, so by the euclidean division, the polynomials of degree smaller than 2 give a set of representatives of the cosets of I. The operations of the factor ring can be given, using these representative elements:
$(a+bx+I)+(c+dx+I)=(a+c)+(b+d)x+I$,
$(a+bx+I)(c+dx+I)=ac+(ad+bc)x+bdx^2+I=ac+(ad+bc)x-bd+bd(x^2+1)+I=(ac-bd)+(ad+bc)x+I$.
It follows that the map $\psi : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$, $\psi : a+bx+I \mapsto a+bi$ is bijective and preserves the operations, so it is an isomorphism.
(*Another way to prove the isomorphism is using the homomorphism theorem:* $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $p(x) \mapsto p(i)$ *is a homomorphism, and* $a+bx \mapsto a+bi$ *shows that it is surjective. The kernel is easily shown to be* I, *so* $\mathbb{R}[x]/I = \mathbb{R}[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = \mathbb{C}$.)
Let us look now at the other case, when we factor the ring of complex polynomials. The elements of the factor ring $\mathbb{C}[x]/(x^2+1)$ can be identified with the set of representatives of the cosets of $I=(x^2+1)$, that is, with the set $\{u+vx \mid u,v \in \mathbb{C}\}$, where the addition is done naturally, and in the multiplication we substitute x^2 by -1, since $x^2+1=0$ in the factor ring. It follows that the factor ring is a two-dimensional vector space over $\mathbb{C}$. Furthermore every ideal of $\mathbb{C}[x]/(x^2+1)$ is also a subspace, since it is closed under multiplication by the constant polynomials. This implies that every nontrivial, proper ideal of the factor ring is one-dimensional as a vector space. If $u^2+v^2 \neq 0$ then $1=(u+vx)\frac{1}{u^2+v^2}(u-vx)$ is in the ideal generated by $u+vx$ so the latter can only be the full factor ring. If $u^2+v^2=(u+vi)(u-vi)=0$, then $u=\pm vi \Rightarrow u+vx=v(x\pm i)$, so every nontrivial ideal contains one of $x+i$ or $x-i$. The scalar multiples of any of these two form a one-dimensional, thus maximal ideal ($(x+i)(u+vx)=(u+vi)x+(ui-v)=(u+vi)(x+i)$ and similarly $(x-i)(u+vx)=(u-vi)x+(-v-ui)=(u-vi)(x-i)$, so these subspaces are, indeed, ideals), hence apart from the trivial ideal and $\mathbb{R}[x]/I$, these two are the only ideals of the factor ring. We still need to verify that these two ideals do not coincide. If they did, then this ideal would contain both $x+i$ and $x-i$, so $1=-\frac{i}{2}((x+i)-(x-i))$ would also be in the ideal, thus this ideal would be the whole factor ring, leading to a contradiction.

4. *Prove that* $K[x]/(x-c) \cong K$ *for any* $c \in K$.

Solution: Consider the ring homomorphism $\varphi : K[x] \to K$, $p(x) \mapsto p(c)$. It is surjective since for every $a \in K$ the constant polynomial a is mapped to a. The kernel of φ is $\{p(x) \in K[x] \mid p(c)=0\} = \{(x-c)q(x) \mid q(x) \in K[x]\}$, which is the ideal $(x-c)$ generated by $x-c$. So $K[x]/(x-c) = K[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = K$ by the homomorphism theorem.

5. *a) Prove that* $K := \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{Q}$ *is a subring of* $\mathbb{R}$, *and* K *is actually a field.*
b) Prove that the field K *defined in part a) is isomorphic to the factor ring* $\mathbb{Q}[x]/(x^2-2)$.

Solution: a) $0=0+0\sqrt{2} \in K$, and for $a,b,c,d \in \mathbb{Q}$,
$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2} \in K$,
$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2} \in K$, and
$1/(a+b\sqrt{2})=(a-b\sqrt{2})/(a^2-2b^2)=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2} \in K$.
In the latter $a^2-2b^2 \neq 0$ if $(a,b) \neq (0,0)$ because $\sqrt{2}$ is irrational. So K is a subring of $\mathbb{R}$, and for every nonzero element of K, the multiplicative inverse (in $\mathbb{R}$) is also in

K, so K is a field.

b) Let $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ be the substitution map $p(x) \mapsto p(\sqrt{2})$. This is a ring homomorphism, and $\operatorname{Im}\varphi \le K$, since for any polynomial $p(\sqrt{2}) = a_n\sqrt{2}^n + \ldots + a_1\sqrt{2} + a_0 = \sum_{k\ even} a_k 2^{k/2} + \sum_{k\ odd} a_k 2^{(k-1)/2}\sqrt{2} \in K$. On the other hand, $\varphi(a+bx) = a + b\sqrt{2}$ shows that $\operatorname{Im}\varphi = K$.
The kernel of φ consists of those polynomials of $\mathbb{Q}[x]$, which have $\sqrt{2}$ as a root. Suppose that $p(x)$ is such a polynomial. If we divide $p(x)$ by x^2-2 then we get $p(x) = (x^2-2)q(x) + r(x)$, where $r(x) = ax+b$ for some $a, b \in \mathbb{Q}$, and $r(\sqrt{2}) = p(\sqrt{2}) - 0q(\sqrt{2}) = 0$. Since $\sqrt{2}$ is irrational, $a = b = 0$, so $p(x) \in (x^2-2)$. This proves that $\operatorname{Ker}\varphi = (x^2-2)$, so $\mathbb{Q}[x]/(x^2-2) = \mathbb{Q}[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = K$.

6. *Prove that every ring R can be embedded into a ring R_1 with identity as an ideal by the following construction (the Dorroh extension of R).*

$$R_1 = \{(r,n) \mid r \in R,\ n \in \mathbb{Z}\}$$
$$(r,n) + (s,m) = (r+s, n+m)$$
$$(r,n)(s,m) = (rs + ns + mr, nm)$$

Solution: As an additive group, this construction gives the direct product of $(R,+)$ and $(\mathbb{Z},+)$, so $(R_1,+)$ is an abelian group. For R_1 to be a ring, we only need to prove that the multiplication is associative, and that distributivity holds in both orders. Note that nr is defined as the n-term sum $r + r + \ldots + r$ if $r \in R$ and $n \in \mathbb{Z}$, $n > 0$, furthermore, $(-n)r := -(nr)$ and $0r = 0$, so it follows from the distributivity and the properties of the additive inverse that for $n, m \in \mathbb{Z}$ and $r, s \in R$, $n(mr) = (nm)r =)mn)r = m(nr)$, and $(nr)s = n(rs) = r(ns)$.

$$\begin{aligned}((r,n)(s,m))(t,k) &= (rs+ns+mr, nm)(t,k)\\ &= (rst + nst + mrt + nmt + krs + nks + mkr, nmk)\\ (r,n)((s,m)(t,k)) &= (r,n)(st + mt + ks, mk)\\ &= (rst + mrt + krs + nst + nmt + nks + mkr, nmk)\end{aligned}$$
$$\Rightarrow\ ((r,n)(s,m))(t,k) = (r,n)((s,m)(t,k))$$
$$((r,n)+(s,m))(t,k) = (r+s, n+m)(t,k) = (rt + st + nt + mt + kr + ks, nk + mk)$$
$$(r,n)(t,k) + (s,m)(t,k) = (rt + nt + kr, nk) + (st + mt + ks, mk)$$
$$\Rightarrow\ ((r,n)+(s,m))(t,k) = (r,n)(t,k) + (s,m)(t,k)$$
$$(r,n)((s,m)+(t,k)) = (r,n)(s+t, m+k) = (rs + rt + ns + nt + mr + kr, nm + nk)$$
$$(r,n)(s,m) + (r,n)(t,k) = (rs + ns + mr, nm) + (rt + nt + kr, nk)$$
$$\Rightarrow\ (r,n)((s,m)+(t,k)) = (r,n)(s,m) + (r,n)(t,k)$$

In R_1 the element $(0,1)$ is an identity: $(r,n)(0,1) = (r0 + n0 + 1r, n1) = (r,n)$ and $(0,1)(r,n) = (0r + 1r + n0, 1n) = (r,n)$.
The subset $\tilde{R} = \{(r,0) \mid r \in R\}$ is an ideal: $(0,0) \in \tilde{R}$, $(r,0) - (s,0) = (r-s, 0) \in \tilde{R}$, $(r,0)(s,m) = (rs + 0s + mr, 0m) = (rs + mr, 0) \in \tilde{R}$ and $(s,m)(r,0) = (sr + mr + 0s, m0) = (sr + mr, 0) \in \tilde{R}$.
Finally, $\tilde{R} \cong R$ by the bijection $(r,0) \mapsto r$, since $(r,0) + (s,0) = (r+s, 0)$ and $(r,0)(s,0) = (rs + 0s + 0r, 0 \cdot 0) = (rs, 0)$.

7. *Let $R = 2\mathbb{Z}$ be the ring of even integers, which is an ideal of $\mathbb{Z}$, a ring with identity. Show that the Dorroh extension R_1 of R defined in problem 3 is not isomorphic to $\mathbb{Z}$.*

Solution: Both $\mathbb{Z}$ and R_1 are rings with identity that contain $2\mathbb{Z}$ as an ideal. Both have a unique identity element, but in $\mathbb{Z}$ this generates the whole ring as a subring, and $(0,1)$ only generates $\{(0,n) \,|\, n \in \mathbb{Z}\}$ in R_1, so the two rings cannot be isomorphic.

HW1. *Let R be a commutative ring, $I \lhd R$ and $S \leq R$. Prove that $SI \lhd R$, but it is not necessarily true if R is not commutative (try to give a counterexample in $R = K^{n \times n}$).*

HW2. *Let K be a field and let R be the ring of upper triangular $n \times n$ matrices over K. Prove that the elements of R with 0 diagonal elements form an ideal in R (call it J). Show that the factor ring R/I is commutative. (Hint: find a homomorphism of R to a commutative ring with kernel J.)*