Additional Exercises:

① Let $\varphi: R \to S$ be a ring hom. We have already shown (in the gp theory part of the course) that $\ker\varphi$ is a subgp of R.

- $\ker\varphi$ is an ideal: Let $a \in R$, $k \in \ker\varphi$. Then:
  $\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)\cdot 0 = 0 \Rightarrow ak \in \ker\varphi$. Similarly,
  $\varphi(ka) = \varphi(k)\varphi(a) = 0 \cdot \varphi(a) = 0 \Rightarrow ka \in \ker\varphi$.

Therefore, $\ker\varphi$ is an ideal.

② (a) I is an ideal of R: We first show I is a subgp of R:

- $(0,0) \in K \Rightarrow 0 \in I$.
- Let $a, b \in I$. Then $\exists\, s_1, s_2 \in S$ s.t. $(a, s_1), (b, s_2) \in K$. Since K is a subgp, $(a+b, s_1+s_2) \in K \Rightarrow a+b \in I$.
- $a \in I \Rightarrow \exists\, s \in S$ s.t. $(a,s) \in K$. K a subgp, so $(-a, -s) \in K$, & thus $-a \in I$.

To show I is an ideal, let $r \in R$ & $a \in I$. Then $\exists\, s \in S$ s.t. $(a,s) \in K$. K is an ideal, so $(r,1)(a,s) = (ra, s) \in K$, so $ra \in I$.

The proof that J is an ideal of S is analogous.

(b) Let $(a,b) \in K$. Then $a \in I$ & $b \in J$, by def, so $(a,b) \in I \times J$. Thus $K \subseteq I \times J$.

(c) Suppose $r \in I$ & $s \in J$. Then $\exists\, s' \in S$, $r' \in R$ s.t. $(r,s'), (r',s) \in K$.
Then $(1_R, s)(r, s') = (r, ss') \in K$, &
$(1_R, s')(r', s) = (r', ss') \in K$,
$\Rightarrow (r, ss') - (r', ss') = (r - r', 0) \in K$. Thus $(r-r', 0) + (r', s) = (r, s) \in K$, and $I \times J = K$.

③ If $M = M_1 \times S$, then $R \times S/M \cong R/M_1$, an integral domain b/c M_1 a max'l ideal of R, so M max'l in $R \times S$. Similarly if $M = R \times M_2$, then M is max'l in $R \times S$.

To show the other direction, assume M is max'l in $R \times S$. By the previous problem, $\exists$ ideals $I \subseteq R$ & $J \subseteq S$ s.t. $M = I \times J$. Thus $R \times S/M \cong R/I \times S/J$. But this product is an integral domain $\Leftrightarrow$ one factor is trivial & the other is an integral domain. Thus either $I = R$ or $J = S$. If $I = R$, then $J \subseteq S$ is maximal, & if $J = S$, then $I \subseteq R$ is max'l, as desired.

④(a) Let $\varphi: \mathbb{C} \to \mathbb{C}$ be defined by $\varphi(a+bi) = a-bi$.
We first show φ is a gp hom:
$\varphi((a+bi)+(c+di)) = \varphi((a+c)+(b+d)i) = (a+c)-(b+d)i$
$= a-bi+c-di = \varphi(a+bi)+\varphi(c+di)$.
We next show φ is a ring hom:
$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i)$
$= (ac-bd)-(ad+bc)i$
$\varphi(a+bi)\varphi(c+di) = (a-bi)(c-di)$
$= (ac-bd)-(ad+bc)i$
Since these are equal, φ is a ring hom.

(b) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_i \in \mathbb{R}$.
Then $f(\varphi(\alpha)) = a_n(\varphi(\alpha))^n + a_{n-1}(\varphi(\alpha))^{n-1} + \cdots + a_0$.
Since φ is a ring hom, $(\varphi(\alpha))^i = \varphi(\alpha^i)$, so
$f(\varphi(\alpha)) = a_n\varphi(\alpha^n) + a_{n-1}\varphi(\alpha^{n-1}) + \cdots + a_0$.
$a_i \in \mathbb{R}$, so $\varphi(a_i) = a_i$, thus,
$f(\varphi(\alpha)) = \varphi(a_n)\varphi(\alpha^n) + \varphi(a_{n-1})\varphi(\alpha^{n-1}) + \cdots + \varphi(a_0)$, & since φ a ring hom,
$= \varphi(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0)$, & since $f(\alpha)=0$
$= \varphi(0)$
$= 0$.
Thus $\varphi(\alpha)$ is a root of f.

(c) Suppose $\deg f(x) > 1$, & let $\alpha \in \mathbb{C}$ s.t. $f(\alpha)=0$. By (b), $\varphi(\alpha)$ is also a root of $f(x)$.
Let $g(x) = (x-\alpha)(x-\varphi(\alpha)) \in \mathbb{R}[x]$. Then $\exists r(x), q(x) \in \mathbb{R}[x]$ with $r(x)=0$ or $\deg r(x) < \deg g(x) = 2$, s.t
$f(x) = g(x)q(x) + r(x)$.
Since α & $\varphi(\alpha)$ are roots of both $f(x)$ & $g(x)$, we have
$0 = f(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$ &
$0 = f(\varphi(\alpha)) = 0 \cdot q(\varphi(\alpha)) + r(\varphi(\alpha)) = r(\varphi(\alpha))$.
But $\deg r(x) < 2$, so if α & $\varphi(\alpha)$ are both roots of $r(x)$, then $\alpha = \varphi(\alpha)$, or $r(x) = 0$. If $\alpha = \varphi(\alpha)$, then $\alpha \in \mathbb{R}$, and so $f(x)$ has a root in $\mathbb{R}$. Thus $f(x)$ is reducible over $\mathbb{R}$. Otherwise, $r(x)=0$, so $g(x)$ divides $f(x)$, i.e. $g(x)q(x) = f(x)$. If $\deg q(x) > 1$, then $f(x)$ is reducible. If $\deg q(x) = 0$, then $f(x)$ is a constant multiple of $g(x)$, so in particular, $\deg f(x) = 2$.
Therefore, every irred. poly in $\mathbb{R}[x]$ has degree 1 or 2.

⑤ Consider the evaluation hom. $\varphi_i: \mathbb{R}[x] \to \mathbb{C}$ defined by $\varphi_i(f(x)) = f(i)$.
- $\ker \varphi_i = (x^2+1)$: We will show both inclusions.
First, $(i)^2+1 = 0$, so $x^2+1 \in \ker\varphi_i$. Since (x^2+1) is the smallest ideal containing x^2+1 (& $\ker\varphi_i$ is an ideal), $(x^2+1) \subseteq \ker\varphi_i$.
Next, let $g(x) \in \ker\varphi_i$. Then i is a root of $g(x)$, & by #4b, so is $-i$. Moreover, in #4c you showed that $(x-i)(x-(-i)) = x^2+1$ divides $g(x)$. Thus, $g(x) \in (x^2+1)$ & so $\ker\varphi_i \subseteq (x^2+1)$.
- φ_i is surjective: Let $a+bi \in \mathbb{C}$. Then $a+bx \in \mathbb{R}[x]$, & $\varphi_i(a+bx) = a+bi$.

Thus, by the 1st Isom. Thm. for Rings,
$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

Exercises 26:

(20) $\varphi_p: R \to R$, $\varphi_p(a) = a^p$.

- φ_p is a gp hom: Let $a, b \in R$. Then $\varphi(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$. $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, and for all $0 < i < p$, p divides $\binom{p}{i}$: $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$, so $i \cdot \binom{p}{i} = p \cdot \binom{p-1}{i-1}$. Thus, p divides $i \cdot \binom{p}{i}$. Since p is prime, either p divides i or p divides $\binom{p}{i}$. $i < p$, so p does not divide i. Thus p divides $\binom{p}{i}$, as desired.

  Since $\operatorname{char} R = p$, $pz = 0$ for all $z \in R$. Thus $\binom{p}{i} a^{p-i} b^i = 0$ for all $0 < i < p$.

- φ_p is a ring hom:
  $\varphi_p(ab) = (ab)^p = a^p b^p = \varphi_p(a)\varphi_p(b)$.
  (R is commutative)

(22) (a) We know $Q(N)$ is a subgp of $Q(R)$. Let $s \in Q(R)$ & $m \in Q(N)$. Then $\exists\, r \in R$ & $n \in N$ s.t. $Q(r) = s$ & $Q(n) = m$.
So, $sm = Q(r)Q(n) = Q(rn)$, & $rn \in N$ b/c N is an ideal.
Thus $sm \in Q(N)$, & so $Q(N)$ is an ideal.

(b) Consider the inclusion homomorphism $Q: \mathbb{Z} \to \mathbb{Q}$ defined by $Q(n) = n$. Then $2\mathbb{Z} \leq \mathbb{Z}$ is an ideal, but $Q(2\mathbb{Z}) = 2\mathbb{Z}$ is not an ideal of $\mathbb{Q}$: since $\mathbb{Q}$ is a field, its only ideals are (0) & $\mathbb{Q}$, neither of which is $2\mathbb{Z}$.

(c) Let N' be an ideal of R'. We know $Q^{-1}(N')$ is a subgp of R. Let $r \in R$ & $n \in Q^{-1}(N')$. Then
$Q(rn) = Q(r)Q(n) \in N'$ since $Q(n) \in N'$ & $Q(r) \in R'$.
Thus, $rn \in Q^{-1}(N')$. This same argument works if N' is an ideal of $Q(R)$, as well.

(25) We know that $+$ & $\cdot$ are well-defined, & that $(R/N, +)$ is an abelian gp.

- $\cdot$ is assoc: Let $a+N, b+N, c+N \in R/N$. Then
  $((a+N)(b+N))(c+N) = (ab+N)(c+N) = (ab)c + N = a(bc) + N = (a+N)(bc)+N) = (a+N)((b+N)(c+N))$ ✓
- Left distributive law: Let $a+N, b+N, c+N \in R/N$.
  $(a+N)[(b+N)+(c+N)] = (a+N)((b+c)+N)$
  $= (a(b+c)) + N$
  $= (ab+ac) + N$
  $= (ab+N) + (ac+N)$ ✓

The right distributive law is similar.
Therefore, R/N is a ring.
Consider $1+N \in R/N$, where 1 is unity in R. Then $\forall\, a+N \in R/N$,
$(a+N)(1+N) = a \cdot 1 + N = a + N = 1 \cdot a + N = (1+N)(a+N)$, so
$1+N$ is unity in R/N.

(26) $I_a = \{x \in R \mid ax = 0\}$.
We first show I_a is a subgp under $+$:

- closure: Let $x, y \in I_a$. Then $a(x+y) = ax + ay = 0 + 0 = 0$, so $x+y \in I_a$.
- identity: $0 \cdot a = 0$, so $0 \in I_a$.
- inverses: Let $x \in I_a$. Then $(-x)(a) = -(xa) = -0 = 0$, so $-x \in I_a$.

Thus I_a is a subgp. Additionally, let $x \in I_a$ & let $r \in R$. Then $(rx)(a) = r(xa) = r \cdot 0 = 0$, so $rx \in I_a$. Therefore, I_a is an ideal of R.

(30) Let $N = \{a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{Z}^+\}$ be the nilradical of R.
We first show N is a subgp of R:
- Closure: Let $a, b \in N$. Then $\exists\, n, m \in \mathbb{Z}^+$ s.t. $a^n = b^m = 0$.
  Consider $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^{n+m-i} b^i$. For every $0 \le i \le n+m$, either $n+m-i \ge n$ or $i \ge m$. In the first case, $a^{n+m-i} = 0$, & in the second case, $b^i = 0$. In either case, $\binom{n+m}{i} a^{n+m-i} b^i = 0$, so $(a+b)^{n+m} = 0$. & $a+b \in N$.
- Identity: $0^1 = 0$, so $0 \in N$.
- Inverses: Let $a \in N$. Then $\exists\, n \in \mathbb{Z}^+$ s.t. $a^n = 0$. $(-a)^n = -a^n = -0 = 0$, so $-a \in N$.

Thus N is a subgp. Additionally, let $r \in R$, $a \in N$. Then $\exists\, n \in \mathbb{Z}^+$ s.t. $a^n = 0$. $(ra)^n = r^n a^n = r^n \cdot 0^0 = 0$, so $ra \in N$. Therefore N is an ideal of R.

(33) Let $a \in R$. Then $a + N \in R/N$, & since the nilradical of R/N is R/N there is some $n \in \mathbb{Z}^+$ s.t. $(a+N)^n = N$ (b/c N is $0_{R/N}$).
Thus $a^n + N = N$, so $a^n \in N$. Since every elt of N is nilpotent, $\exists\, m \in \mathbb{Z}^+$ s.t. $(a^n)^m = 0$. Therefore a is nilpotent. Since $a \in R$ was arbitrary, this shows that every elt of R is nilpotent, & thus the nilradical of R is R.

(34) $\sqrt{N} = \{a \in R \mid a^n \in N \text{ for some } n \in \mathbb{Z}^+\}$.
We first show $\sqrt{N}$ is a subgp of R:
- closure: Let $a, b \in \sqrt{N}$. Then $\exists\, n, m \in \mathbb{Z}^+$ s.t. $a^n \in N$ and $b^m \in N$.
  Then $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^{n+m-i} b^i$.
  For every $0 \le i \le n+m$, either $n+m-i \ge n$ or $i \ge m$. In the first case $a^{n+m-i} \in N$, & since N is an ideal, $\binom{n+m}{i} a^{n+m-i} b^i \in N$. In the second case, $b^i \in N$ & since N is an ideal, $\binom{n+m}{i} a^{n+m-i} b^i \in N$. Thus $(a+b)^{n+m}$ is a sum of elts in N, & so $(a+b)^{n+m} \in N$. Therefore, $a+b \in \sqrt{N}$.
- identity: N is a subgp of R, so $0 \in N$. Thus $0 \in \sqrt{N}$.
- inverses: Let $a \in N$. Then $\exists\, n \in \mathbb{Z}^+$ s.t. $a^n \in N$. $(-a)^n = -a^n$), & since N is a subgp, $-(a^n) \in N$. Thus $-a \in \sqrt{N}$.

Therefore $\sqrt{N}$ is a subgp of R. Additionally, let $r \in R$ & $a \in \sqrt{N}$. Then $\exists\, n \in \mathbb{Z}^+$ s.t. $a^n \in N$.
$(ra)^n = r^n a^n \in N$ b/c $a^n \in N$ & N is an ideal. Thus $ra \in \sqrt{N}$.
Therefore, $\sqrt{N}$ is an ideal of R.