Images and kernels Some Theorems and some Homework

1. ~~*Fill in the missing line of the proof*~~

Prove: Theorem 75: If *R* and *S* are rings, and $f: R \to S$ is a ring homomorphism, then $f(0_R) = 0_S$ where 0_R is the additive identity in *R*, and 0_S is the additive identity in *S*.

Proof: $0_R + 0_R = 0_R$

So $f(0_R + 0_R) = f(0_R)$ because *f* is a well defined function.

And $f(0_R + 0_R) = f(0_R) + f(0_R)$ because ________________________________

So $f(0_R) + f(0_R) = f(0_R)$

So $f(0_R) + f(0_R) + (-f(0_R)) = f(0_R) + (-f(0_R))$ because *S* is a ring and elements in *S* have additive inverses.

Thus $f(0_R) + 0_S = 0_S$, and therefore $f(0_R) = 0_S$

2. ~~*Fill in the missing lines in the proof*~~

Prove Theorem 76: If *R* is a ring that has a multiplicative identity 1_R, and *S* is a field whose multiplicative identity is 1_S, and $f: R \to S$ is a ring homomorphism and there is some $a \in R$ such that $f(a) \neq 0$, then $f(1_R) = 1_S$

Proof: $a \cdot 1_R = a$

So $f(a \cdot 1_R) = f(a)$

And __________________________ because *f* is a homomorphism

So $f(a) \cdot f(1_R) = f(a)$

So $\left(f(a)\right)^{-1} \cdot f(a) \cdot f(1_R) = \left(f(a)\right)^{-1} \cdot f(a)$ because *S* is a _________________and elements in *S* have -

____

Thus__________________, and therefore $f(1_R) = 1_S$

3. ~~*Fill in the missing line of the proof*~~

Prove Theorem 77: If *R* and *S* are rings, and $f: R \to S$ is a ring homomorphism and $a \in R$, then $f(-a) = -f(a)$

Proof: $a + -a = 0_R$

So, $f(a + -a) = f(0_R)$

And ____________________ because *f* is a homomorphism

So $f(a) + f(-a) = f(0_R)$

And $f(a) + f(-a) = 0_S$ by theorem 75

So $-f(a) + f(a) + f(-a) = -f(a) + 0_S$

And $0_S + f(-a) = -f(a)$

Therefore $f(-a) = -f(a)$

4. Proving Theorem 53/78: If R and S are rings, and $f: R \to S$ is a ring homomorphism, then $f(R) = \{f(x) \mid x \in R\} \subseteq S$ is a subring of S.

Proof:

first: show that $f(R)$ *is closed under addition*

Let $f(a),(b) \in f(R)$

then $a, b \in R$

and $f(a) + f(b) = f(a+b)$ because f is a homomorphism,

and $a+b \in R$, so $f(a+b) \in f(R)$

So $f(a) + f(b) \in f(R)$

second: show has $f(R)$ *additive inverses*

Let $f(a) \in R$

then $a \in R$ and therefore $-a \in R$, so $f(-a) \in f(R)$

by theorem 77, we know $f(-a) = -f(a)$, so $-f(a) \in f(R)$

third: show $f(R)$ *is closed under multiplication*

Finish the proof of theorem 53/78 by doing the third part:

show $f(R)$ *is closed under multiplication*

5. Proving Theorem 79: If R and S are rings, and $f: R \to S$ is a ring homomorphism, then $\ker(f) \subseteq R$ is an ideal in R.

Proof:

first: prove $\ker(f)$ *is closed under addition*

Let $a, b \in \ker(f)$

then $f(a) = f(b) = 0$

And $f(a+b) = f(a) + f(b)$ because f is a homomorphism

Therefore $f(a+b) = f(a) + f(b) = 0 + 0 = 0$

so $a + b \in \ker(f)$

second: prove $\ker(f)$ *includes additive inverses*

Let $a \in \ker(f)$

$-a \in R$ and $f(-a) = -f(a)$ by theorem 77

So $f(-a) = -f(a) = -0 = 0$

Therefore $-a \in \ker(f)$

Finish the proof of theorem 79 by showing the third part:

prove that $\ker(f)$ *multiplicatively absorbs elements of R*

6. Proving Theorem 80 (First Isomorphism Theorem)**:** If R and S are rings, and $f : R \to S$ is a surjective (onto) ring homomorphism, then $R/\ker(f) \cong S$ with isomorphism $\phi(r+\ker(f)) = f(r)$ where $r+\ker(f) \in R/(\ker(f))$

Proof: First show ϕ is a well-defined function:
Suppose $r+\ker(f), s+\ker(f) \in R/\ker(f)$ such that $r+\ker(f) = s+\ker(f)$
then $s-r = i \in \ker(f)$
So $f(s-r) = f(s)+f(-r) = f(s)+-f(r)$ because f is a homomorphism
but also $f(s-r) = f(i) = 0$
So $f(s)-f(r) = 0$
And thus $f(s) = f(r)$
Therefore $\phi(s+\ker(f)) = f(s) = f(r) = \phi(r+\ker(f))$
and hence, f is a well-defined function

Second, show ϕ is onto:
Let $s \in S$
Then, because f is surjective, there exists an $r \in R$ such that $f(r) = s$
Now $r+\ker(f) \in R/\ker(f)$
and $\phi(r+\ker(f)) = f(r) = s$
so ϕ is onto.

Third, show ϕ is one-to-one
Let $r+\ker(f), s+\ker(f) \in R/\ker(f)$ such that $\phi(r+\ker(f)) = \phi(s+\ker(f))$
Then $f(r) = f(s)$
So $f(r)-f(s) = 0$
But $f(r)-f(s) = f(r)+f(-s) = f(r+-s) = f(r-s)$
So $f(r-s) = 0$
And by definition, $r-s \in \ker(f)$
And therefore $r \equiv s \pmod{\ker(f)}$
so $r+\ker(f) = s+\ker(f)$
And therefore, ϕ is one=to-one.

Fourth show ϕ preserves addition:
Let $r+\ker(f), s+\ker(f) \in R/\ker(f)$
Then $\phi((r+\ker(f))+(s+\ker(f))) = \phi((r+s)+\ker(f)) = f(r+s)$
And $\phi(r+\ker(f))+\phi(s+\ker(f)) = f(r)+f(s)$
and f is a homomorphism, so $f(r+s) = f(r)+f(s)$
Therefore (by the transitive property) $\phi((r+\ker(f))+(s+\ker(f))) = \phi(r+\ker(f))+\phi(s+\ker(f))$
So ϕ preserves addition.

Fourth show ϕ preserves multiplication:
$\phi((r+\ker(f))\cdot(s+\ker(f))) = \phi((r\cdot s)+\ker(f)) = f(r\cdot s)$
And $\phi(r+\ker(f))\cdot\phi(s+\ker(f)) = f(r)\cdot f(s)$
and f is a homomorphism, so $f(r\cdot s) = f(r)\cdot f(s)$
Therefore (by the transitive property) $\phi((r+\ker(f))\cdot(s+\ker(f))) = \phi(r+\ker(f))\cdot\phi(s+\ker(f))$
So ϕ preserves multiplication.

7. Proving Theorem 81: If $f(x) \in F[x]$ is an irreducible polynomial with coefficients in the field *F*, then $F[x]/(f(x))$ is a field.

By theorem 74, we already know that $F[x]/(f(x))$ is a ring.

Commutativity:
Because *F* is a field, it is commutative, and since *x* by definition commutes with every element of *F*, we can conclude that $F[x]$ is commutative.
To simplify the notation, we will use the notation $[g]_f = g(x)+\left(f(x)\right) \in F[x]/\left(f(x)\right)$ for any
By theorem 73, if $[g]_f[h]_f \in F[x]/\left(f(x)\right)$,
then $[g]_f \cdot [h]_f = [g \cdot h]_f$
Using commutativity of $F[x]$, $[g]_f \cdot [h]_f = [g \cdot h]_f = [h \cdot g]_f = [h]_f \cdot [g]_f$
Thus $F[x]/(f(x))$ is a commutative ring.

Multiplicative identity:
F has a multiplicative identity 1, and that identity will also be the multiplicative identity for $F[x]$
Let $[g]_f = g(x)+\left(f(x)\right) \in F[x]/\left(f(x)\right)$, then
$[g]_f \cdot [1]_f = [g \cdot 1]_f = [g]_f = [1 \cdot g]_f = [1]_f \cdot [g]_f$
so $[1]_f = 1+\left(f(x)\right)$ is the multiplicative identity for $F[x]/(f(x))$

All non-zero elements are units
Let $[g]_f = g(x)+\left(f(x)\right) \in F[x]/\left(f(x)\right)$, such that $[g]_f \neq [0]_f$, which means $g(x) \notin \left(f(x)\right)$ and $f(x) \nmid g(x)$
Then $g(x)$ and $f(x)$ have a greatest common divisor, $d(x)$ in $F[x]$, and by theorem 58, there exist polynomials $u(x), v(x) \in F[x]$ such that $d(x) = u(x)f(x) + v(x)g(x)$
Now, $d(x)$ is a divisor of $f(x)$, and because $f(x)$ is irreducible, then either $d(x)=1$, or $d(x)$ is an associate of $f(x)$

> Suppose $d(x)$ is an associate of $f(x)$
> Then $d(x) = c \cdot f(x)$ where $c \in F$ and $c \neq 0$
> But $d(x) = c \cdot f(x)$ is also a divisor of $g(x)$, which means that $f(x) \mid g(x)$, but this contradicts $[g]_f \neq [0]_f$

Therefore, $d(x)=1$
Thus we get $1 = u(x)f(x) + v(x)g(x)$
and $u(x)f(x) \in \left(f(x)\right)$
Therefore $v(x)g(x) = 1 + u(x)f(x) \in 1 + \left(f(x)\right) = [1]_f$
And hence $[v]_f \cdot [g]_f = [1]_f$
Therefore, $[g]_f$ is a unit, and $F[x]/\left(f(x)\right)$ is a field.

9. Proving Theorem 82: If $f(x) \in F[x]$ is an irreducible polynomial with coefficients in a field F such that $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, and $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ then $\phi : F[x]/(f(x)) \to F(\alpha)$ defined by $\phi\big(g(x) + (f(x))\big) = g(\alpha)$ is an isomorphism and $F[x]/\big(f(x)\big) \cong F(\alpha)$.

Proof:

We will begin by defining a function $\psi : F[x] \to F(\alpha)$ such that $\psi(g(x)) = g(\alpha)$

Note that for any $g(x) \in F[x]$, the number $g(\alpha)$ is computed by adding, subtracting and multiplying elements in $F(\alpha)$ (which is a field that contains α and the elements of F), so $g(\alpha) \in F(\alpha)$ (so ψ is a well defined function).

Let $g(x), h(x) \in F[x]$

Then $\psi(g(x) + h(x)) = g(\alpha) + h(\alpha) = \psi(g(x)) + \psi(h(x))$

And $\psi(g(x) \cdot h(x)) = g(\alpha) \cdot h(\alpha) = \psi(g(x)) \cdot \psi(h(x))$

So ψ is a homomorphism

Let $K = \psi(F[x]) \subseteq F(\alpha)$ be the range of ψ

Then, by the first isomorphism theorem, $F[x]/\ker(\psi) \cong K$, where $\phi\big(g(x) + \ker(\psi)\big) = \psi(g(x)) = g(\alpha)$ is the isomorphism. (1)

Next, we will show that $\ker(\psi) = \big(f(x)\big)$:

We know $\psi(f(x)) = f(\alpha) = 0$, so $f(x) \in \ker(\psi)$

Also, if $h(x)f(x) \in \big(f(x)\big)$, then $\psi(h(x)f(x)) = h(\alpha)f(\alpha) = h(\alpha) \cdot 0 = 0$, so $\big(f(x)\big) \subseteq \ker(\psi)$

Let $g(x) \in \ker(\psi)$, so $\psi(g(x)) = g(\alpha) = 0$

Then $g(x)$ and $f(x)$ have a greatest common divisor, $d(x)$ in $F[x]$, and by theorem 58, there exist polynomials $u(x), v(x) \in F[x]$ such that $d(x) = u(x)f(x) + v(x)g(x)$ (2)

Now, $d(x)$ is a divisor of $f(x)$, and because $f(x)$ is irreducible, then either $d(x)$ is a non-zero constant, or $d(x)$ is an associate of $f(x)$

We can substitute in α into (2) to get $d(\alpha) = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = u(\alpha) \cdot 0 + v(\alpha) \cdot 0 = 0$, so $d(x)$ cannot be a non-zero constant.

Therefore $d(x) = c \cdot f(x)$ where $c \in F$ and $c \neq 0$

We know that $d(x) \mid g(x)$, so $f(x) \mid g(x)$, so $g(x) \in \big(f(x)\big)$

Therefore $\ker(\psi) \subseteq \big(f(x)\big)$ and hence $\big(f(x)\big) = \ker(\psi)$

Substituting into (1), we have that $F[x]/\big(f(x)\big) \cong K$ where the isomorphism is $\phi\big(g(x) + (f(x))\big) = g(\alpha)$ (3)

By theorem 53/78, we know that K is a ring. Because $\mathbb{Q} \subseteq F \subseteq K \subseteq \mathbb{C}$, we know that K is commutative and contains a multiplicative identity.

Let $a \in K$ such that $a \neq 0$, then $a = \psi(g(x)) = g(\alpha)$ for some $g(x) \in F[x]$

$g(\alpha) \neq 0$ so $g(x) \notin \ker(\psi) = \big(f(x)\big)$, so $[g]_f = g(x) + \big(f(x)\big)$ is a non-zero element of $F[x]/\big(f(x)\big)$

By theorem 77, we know that $F[x]/(f(x))$ is a field, so $[g]_f \neq [0]_f$, has a multiplicative inverse $[h]_f \in F[x]/\big(f(x)\big)$ such that $[g]_f[h]_f = 1_f$

ϕ is a homomorphism, so $\phi([g]_f[h]_f) = \phi([1]_f) = 1 \in K$

and $\phi([g]_f \cdot [h]_f) = \phi([g]_f) \cdot \phi([h]_f) = g(\alpha)h(\alpha) = a \cdot h(\alpha)$

$h(\alpha) \in K$ and $a \cdot h(\alpha) = 1$, so *a* has a multiplicative inverse in *K*.

Therefore every non-zero element of *K* has a multiplicative inverse, and *K* is a field.

Note that if $a \in F$, then $\psi(a) = a \in K$, so $F \subseteq K$

Also note that $\psi(x) = \alpha \in K$

So *K* is a field that includes *F* and includes α and $K = \psi(F[x]) \subseteq F(\alpha)$

But $F(\alpha)$ is defined to be the smallest subfield of $\mathbb{C}$ that contains both *F* and *α*, so $F(\alpha) = K$

Finally, substituting into (3), we conclude that $F[x]/\left(f(x)\right) \cong F(\alpha)$