Exam 3 will be on Monday, November 19, 2018. The syllabus for this exam is Chapter 11, Section 13.1, and Chapter 16 in Judson.

You should be sure to know precise definition of the terms we have used, and you should know precise statements (including all relevant hypotheses) for the main theorems proved. Know the following terms or phrases, including definitions, and results. Some are repeated for convenience from earlier sections.

- A function $f : G \to H$ between groups G and H is a homomorphism if $f(ab) = f(a)f(b)$ for all $a, b \in G$. Some properties of homomorphisms are: $f(1) = 1$, $f(a^{-1}) = (f(a))^{-1}$, $f(a^k) = (f(a))^k$ for all $k \in \mathbb{Z}$.
- A bijective homomorphism $f : G \to H$ is an isomorphism.
- Kernel of a group homomorphism
- Normal subgroup
- Right and left cosets of a subgroup H of a group G.
- The index $[G : H]$ of a subgroup H in a group G.
- Let H be a subgroup of a group G and let $a, b \in G$. Then the following are properties of the cosets of H:
  1. $Ha = H$ if and only if $a \in H$.
  2. $Ha = Hb$ if and only if $ab^{-1} \in H$.
  3. If $a \in Hb$, then $Ha = Hb$.
  4. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.
  5. The distinct right (left) cosets of H are a partition of G, and if the order of G is finite, then the number of right (left) cosets is $|G|/|H|$.
- If G is a group and H is a subgroup, then H is a normal subgroup if $gH = Hg$ for all $g \in G$.
- A subgroup H of G is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.
- If G is a group, then then subgroups $\{1\}$, G and $Z(G) =$ the center of G, are always normal subgroups of G.
- If G is abelian, then every subgroup of G is normal in G.
- If H is a subgroup of index 2 in G, then H is normal in G.
- If K is a normal subgroup of G, then $Ka \cdot Kb = Kab$ is a well defined multiplication of right (=left) cosets. In this case the set $G/K = \{Ka : a \in G\}$ of right (=left) cosets of K forms a group under this multiplication. Some of the properties of this group G/K are:

1. The group operation is $(Ka)(Kb) = Kab$.
2. The identity of G/K is the coset K.
3. The inverse of Ka is Ka^{-1}, i.e., $(Ka)^{-1} = Ka^{-1}$.
4. The exponent rule in G/K is $(Ka)^n = Ka^n$.
5. The order of Ka is the smallest positive power n such that $a^n \in K$.
6. The mapping $\varphi : G \to G/K$ defined by $\varphi(a) = Ka$ is a surjective group homomorphism.
7. If G is abelian, then G/K is abelian.
8. If $G = \langle a \rangle$ is cyclic, then G/K is also cyclic; in fact $G/K = \langle Ka \rangle$
9. If G is finite, then $|G/K| = |G|/|K| = [G : K]$.

- If $\alpha : G \to H$ is a group homomorphism, the (1) $\alpha(G)$ is a subgroup of H, and (2) $\text{Ker}(\alpha)$ is a *normal* subgroup of G.
- ***Isomorphism Theorem for Groups.*** If $\alpha : G \to H$ is a group homomorphism, then $\alpha(G) \cong G/\text{Ker}(\alpha)$.
- Know the criterion for an abelian group G to be the internal direct product of subgroups H and K. Specifically, G is the internal direct sum of H and K provided $HK = \{hk : h \in H, k \in K\}$ and $H \cap K = \{1\}$. In this case G is isomorphic to the external direct product $H \times K$ via the isomorphism $\phi : H \times K \to G$ given by $\phi(h, k) = hk$.
- ***Fundamental Theorem of Finite Abelian Groups.*** Every finite abelian group G is isomorphic to a direct product of cyclic groups of prime power order.
- Ring, commutative ring.
- Subring
- ***Subring Test.*** A subset S of a ring R is a subring if and only if
  1. $0 \in S$.
  2. If $s \in S$ and $t \in S$, then $s + t$, st, and $-s$ are all in S.
- Units in a ring
- Characteristic of a ring.
- Division Ring
- Field
- A ring R is an *integral domain* if R is commutative with identity, $1 \neq 0$, and $ab = 0 \implies a = 0$ or $b = 0$.
- A subring of a field is an integral domain.

- The characteristic of any domain is either 0 or a prime.
- Every finite integral domain is a field.
- An *ideal* of a ring R is an additive subgroup A such that $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$. Thus, to check that a nonempty $A \subset R$ is an ideal, it is necessary to check:
  1. If a, $b \in A$ then $a \pm b \in A$.
  2. If $a \in A$ and $r \in R$, then $ra \in A$ and $ar \in A$.
- Let A be an ideal of the ring R. Then the additive factor group R/A becomes a ring with the multiplication $(r + A)(s + A) = rs + A$. The unity of R/A is $1 + A$, and R/A is commutative if R is commutative (but R/A can be commutative without R being commutative).
- Let A is an ideal of a ring R, then the ideals of R/A are all of the form B/A where B is an ideal of R containing A. (Theorem 4, page 183).
- If R is commutative and $a \in R$, then $Ra = \{ra | r \in R\}$ is an ideal of R called the *principal ideal generated by* a.
- An ideal P of a commutative ring R is a *prime ideal* if $P \neq R$ and P has the property:

  $$\text{If } rs \in P, \text{ then } r \in P \text{ or } s \in P.$$

- An ideal M of a ring R is *maximal* if $M \neq R$ and the only ideals A such that $M \subseteq A \subseteq R$ are $A = M$ and $A = R$.
- The only ideals of a division ring R are $|set0$ and R.
- If R is a commutative ring, an ideal $P \neq R$ is a prime ideal if and only if R/P is an integral domain.
- If R is a commutative ring, an ideal A of R is maximal if and only if R/A is a field.
- If R is a commutative ring, then every maximal ideal is a prime ideal.
- If R is a ring, then the ideals of the matrix ring $M_n(R)$ are all of the form $M_n(A)$ where A is an ideal of R.
- If R and S are rings, a map $\theta : R \to S$ is a *ring homomorphism* if for all r and $r_1 \in R$:
  1. $\theta(r + r_1) = \theta(r) + \theta(r_1)$.
  2. $\theta(rr_1) = \theta(r)\theta(r_1)$.
- If $\theta : R \to S$ is a ring homomorphism, then
  1. $\theta(R)$ is a subring of S.
  2. $\text{Ker}(\theta)$ is an ideal of R.

- ***Isomorphism Theorem for Rings.*** If $\theta : R \to A$ is a ring homomorphism, then $\theta(R) \cong R/\operatorname{Ker}(\theta)$, via the ring isomorphism $\overline{\theta} : R/\operatorname{Ker}(\theta) \to \theta(R)$ given by $\overline{\theta}(r + \operatorname{Ker}(\theta)) = \theta(r)$.
- ***Chinese Remainder Theorem.*** Let A and B be ideals of a ring R.
  1. If $A + B = R$ then $R/(A \cap B) \cong R/A \times R/B$.
  2. If $A + B = R$ and $A \cap B = 0$ then $\cong R/A \times R/B$.
- If m and n are relatively prime, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Here the isomorphism is an isomorphism of rings.

Review Exercises

1. Let N be a normal subgroup of prime index p in a group G. Explain why the quotient group G/N is cyclic.

   ▶ **Solution.** Since $|G/N| = [G : N] = p$, it follows that the order of G/N is prime, and hence is cyclic. (Every group of prime order is cyclic, with any nonidentity element being a generator.) ◀

2. List the cosets of $\langle 7 \rangle$ in $\mathbb{Z}_{16}^*$. Is the quotient group $\mathbb{Z}_{16}^*/\langle 7 \rangle$ cyclic?

   ▶ **Solution.** $\langle 7 \rangle = \{1, 7\}$ since $7^2 = 1$ in $\mathbb{Z}_{16}^*$. Thus, the cosets are $\langle 7 \rangle$, $3\langle 7 \rangle = \{3, 5\}$, $9\langle 7 \rangle = \{9, 15\}$, and $11\langle 7 \rangle = \{11, 13\}$. Since $|\mathbb{Z}_{16}^*/\langle 7 \rangle| = 4$ and $(3\langle 7 \rangle)^2 = 9\langle 7 \rangle \neq \langle 7 \rangle$ it follows that $o(3\langle 7 \rangle) = 4$ so $\mathbb{Z}_{16}^*/\langle 7 \rangle$ is cyclic with generator $3\langle 7 \rangle$. ◀

3. Let $\mathbb{R}$ be the additive group of the real numbers, $\mathbb{Z}$ its cyclic subgroup

   $$\langle 1 \rangle = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

   and let W be the quotient group $\mathbb{R}/\mathbb{Z}$.

   (a) What is the order of the coset $(-2/5) + \mathbb{Z}$ in the group W?

   ▶ **Solution.** Since the group operation is addition, the order of a coset $r + \mathbb{Z}$ in $\mathbb{R}/\mathbb{Z}$ is the smallest positive integer n such that $nr \in \mathbb{Z}$, if there is such a number, otherwise the order is infinite. If $r = -2/5$ then $5r = -2 \in \mathbb{Z}$ and for any integer m smaller than 5, $mr \notin \mathbb{Z}$. Thus, the order of $(-2/5) + \mathbb{Z}$ in the group W is 5. ◀

   (b) Use the fact that $\sqrt{3}$ is irrational to show that the coset $\sqrt{3} + \mathbb{Z}$ does not have finite order in the group W.

   ▶ **Solution.** If $\sqrt{3} + \mathbb{Z}$ has order $n > 0$, then $n\sqrt{3} = m \in \mathbb{Z}$. Thus, $\sqrt{3} = m/n$ is rational. Since $\sqrt{3}$ is not rational, it follows that there is no such n, and hence the order of $\sqrt{3} + \mathbb{Z}$ is infinite. ◀

4. If $G = \mathbb{Z}_6 \times \mathbb{Z}_4$ let $H = \{(0,0),\ (0,2)\}$ and $K = \{(0,0),\ (3,0)\}$.

   (a) Check that H and K are subgroups of G.

   ▶ **Solution.** Since $2(0,\ 2) = (0,\ 0)$ it follows that $H = \langle(0,\ 2)\rangle$ and since $2(3,\ 0) = (0,\ 0)$ it follows that $K = \langle(3,\ 0)\rangle$. Thus, both H and K are cyclic groups of order 2. ◀

   (b) List all of the cosets of H. List all of the cosets of K.

   ▶ **Solution.**

Cosets of H	
$\{(0,\ 0),\ (0,\ 2)\}$	$\{(0,\ 1),\ (0,\ 3)\}$
$\{(1,\ 0),\ (1,\ 2)\}$	$\{(1,\ 1),\ (1,\ 3)\}$
$\{(2,\ 0),\ (2,\ 2)\}$	$\{(2,\ 1),\ (2,\ 3)\}$
$\{(3,\ 0),\ (3,\ 2)\}$	$\{(3,\ 1),\ (3,\ 3)\}$
$\{(4,\ 0),\ (4,\ 2)\}$	$\{(4,\ 1),\ (4,\ 3)\}$
$\{(5,\ 0),\ (5,\ 2)\}$	$\{(5,\ 1),\ (5,\ 3)\}$

Cosets of K	
$\{(0,\ 0),\ (3,\ 0)\}$	$\{(0,\ 1),\ (3,\ 1)\}$
$\{(0,\ 2),\ (3,\ 2)\}$	$\{(0,\ 3),\ (3,\ 3)\}$
$\{(1,\ 0),\ (4,\ 0)\}$	$\{(1,\ 1),\ (4,\ 1)\}$
$\{(1,\ 2),\ (4,\ 2)\}$	$\{(1,\ 3),\ (4,\ 3)\}$
$\{(2,\ 0),\ (5,\ 0)\}$	$\{(2,\ 1),\ (5,\ 1)\}$
$\{(2,\ 2),\ (5,\ 2)\}$	$\{(2,\ 3),\ (5,\ 3)\}$

   ◀

   (c) What is the isomorphism class of G/H?

   ▶ **Solution.** The group $\mathbb{Z}_{12}$ is cyclic of order 12, so it has an element of order 12. The group $\mathbb{Z}_6 \times \mathbb{Z}_2$ has the order of every element divisible by 6 since $6(a,\ b) = (0,\ 0)$ for all $(a,\ b) \in \mathbb{Z}_6 \times \mathbb{Z}_2$. From the coset table for the subgroup H, we see that $6(r,\ 0) = (0,\ 0) \in H$ and $6(r,\ 1) = (0,\ 0) \in H$ for all $r \in \mathbb{Z}_6$. Since these are representatives of all cosets in G/H, it follows that the order of every element of G/H is divisible by 6. Since there is no element of order 12, it follows that G/H must be isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$.

   Since $6(1,\ 1) = (0,\ 2) \notin K$ and since $4(1,\ 1) = (4,\ 0) \notin K$, it follows that the order of $(1,\ 1) + K$ is not 1, 2, 3, 4, or 6. Thus it must be 12 so that G/K is cyclic of order 12, that is, G/K is isomorphic to $\mathbb{Z}_{12}$. ◀

   (d) What is the isomorphism class of G/K?

   ▶ **Solution.** Since $6(1,\ 1) = (0,\ 2) \notin K$ and since $4(1,\ 1) = (4,\ 0) \notin K$, it follows that the order of $(1,\ 1) + K$ is not 1, 2, 3, 4, or 6. Thus it must be 12 so that G/K is cyclic of order 12, that is, G/K is isomorphic to $\mathbb{Z}_{12}$. ◀

5. Give a complete list of the distinct isomorphism classes of abelian groups of order 600.

   ▶ **Solution.** The prime factorization of 600 is $600 = 2^3 \cdot 3 \cdot 5^2$. Thus, by the Fundamental theorem of finite abelian groups, any group of order 600 is a product of an abelian group of order 8, a group of order 3, and an abelian group of order 25. The abelian groups of order 8 are $\mathbb{Z}_8$, $Z_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The only group of order 3

is $\mathbb{Z}_3$, and the abelian groups of order 25 are $\mathbb{Z}_{25}$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$. Thus, there are a total of 6 (up to isomorphism) groups of order 600:

$$\begin{aligned}
\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} &\cong \mathbb{Z}_{600} \\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} &\cong \mathbb{Z}_2 \times \mathbb{Z}_{300} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{150} \\
\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 &\cong \mathbb{Z}_5 \times \mathbb{Z}_{120} \\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 &\cong \mathbb{Z}_{10} \times \mathbb{Z}_{60} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{30}
\end{aligned}$$

In this list, the groups on the left are written as a product of cyclic groups of prime power order. The isomorphic groups on the right are written in what is called *invariant factor form*, which is in the form $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ where $n_i \mid n_{i+1}$ for $1 \leq i < r$. ◀

6. Are the groups $\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{25} \times \mathbb{Z}_{36} \times \mathbb{Z}_{54}$ and $\mathbb{Z}_{50} \times \mathbb{Z}_{108} \times \mathbb{Z}_{450}$ isomorphic?

▶ **Solution.** To answer this, write each of the groups as a product of cyclic groups of prime power order. Note that both groups have the same order, namely, 2,430,000. The first group decomposed as a product of cyclic groups of prime power order gives

$$\mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$$

while the second group decomposes into a product of cyclic groups of prime power order as

$$\mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_9$$

Since these two products do not have the same numbers of factors of each prime power order, they are not isomorphic. ◀

7. What is the isomorphism type of the group $U(20)$ (the group of units of the ring $\mathbb{Z}_{20}$).

▶ **Solution.** $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ which is a group of order 8. Then $\langle 3 \rangle = \{1, 3, 9, 7\}$ and $\langle 11 \rangle = \{1, 11\}$. Thus, $\langle 3 \rangle \cap \langle 11 \rangle = \{1\}$ so $|\langle 3 \rangle \langle 11 \rangle| = 8$. Hence, $U(20) = \langle 3 \rangle \langle 11 \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. ◀

8. Two of the following groups of order 864 are isomorphic. Which are the two?

   (a) $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}$

   (b) $\mathbb{Z}_3 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24}$

   (c) $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9$

▶ **Solution.** As in problem 6, decompose each group into a product of cyclic groups of prime power order:

   (a) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$

(b) $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_3$

(c) $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$

From this, it is clear the groups (a) and (c) are isomorphic, and they are not isomorphic to group (b). ◀

9. Which of the following are subrings of the field $\mathbb{R}$ of real numbers.

(a) $A = \{m + n\sqrt{2} | m, n \in \mathbb{Z} \text{ and } n \text{ is even}\}$

▶ **Solution.** Apply the subring test. Let $a = m + n\sqrt{2}$ and $b = r + s\sqrt{2}$ be arbitrary elements of A. This means that m, n, r, s are in $\mathbb{Z}$ with n and s even. Then $a + b = (m + r) + (n + s)\sqrt{2}$ and $ab = (mr + 2ns) + (ms + nr)\sqrt{2}$. Since n and s are even it follows that $n + s$ and $ms + nr$ are both even. Hence $a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$, and A is closed under addition and multiplication. Next $-a = (-m) + (-n)\sqrt{2}$ and $-n$ is even since n is even. Thus $-a \in A$ for all $a \in A$. Last $1 = 1 + 0\sqrt{2}$ and since 0 is even, we have $1 \in A$. Hence A satisfies all conditions of the subring test, and hence A is a subring of $\mathbb{R}$. ◀

(b) $B = \{m + n\sqrt{2} | m, n \in Z \text{ and } m \text{ is odd}\}$

▶ **Solution.** $a = \sqrt{2} = 0 + 1\sqrt{2} \in B$ but $a + a = 0 + 2\sqrt{2} \notin B$ since 2 is not odd. ◀

10. Consider the following conditions on the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with rational entries. Which conditions below define a commutative ring? If the set is a ring, find all units.

(a) All matrices with $d = a$, $c = b$.

▶ **Solution.** The conditions $d = a$, $c = b$ determine the set A of matrices with entries in $\mathbb{Q}$ of the form $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$. Since $\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}$ it follows that A is closed under addition. Moreover, letting $a = 1$, $b = 0$ shows that the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in A$. Also $-\begin{bmatrix} a & b \\ b & a \end{bmatrix} = \begin{bmatrix} -a & -b \\ -b & -a \end{bmatrix} \in A$. It remains to check that A is closed under multiplication and that multiplication is commutative. But this follows from the calculation:

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + bd & ad + bc \\ ad + bc & ac + bd \end{bmatrix} = \begin{bmatrix} c & d \\ d & c \end{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

◀

(b) All matrices with $a = 0$ and $d = 0$.

▶ **Solution.** The set of such matrices is not closed under multiplication. For a counterexample consider the multiplication

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, it cannot be a ring. ◀

11. An element a of a commutative ring R is called **nilpotent** if $a^n = 0$ for some positive integer n. Prove that if u is a unit and a is nilpotent, then $u - a$ is a unit in R.

▶ **Solution.** Let x be any element of R. Then the distributive law and rules of exponents give the formula

$$(1 - x)(1 + x + x^2 + \cdots + x^k) = 1 - x^{k+1}.$$

If $a \in R$ is nilpotent with $a^n = 0$, then letting $x = a$ in this formula and $k = n - 1$ gives

$$(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1 - a^n = 1.$$

Thus, if a is nilpotent then $1 - a$ is a unit with $(1 - a)^{-1} = (1 + a + a^2 + \cdots + a^{n-1})$. Now let u be any unit and let a be a nilpotent element of R with $a^n = 0$. Then $(au^{-1})^n = a^n u^{-n} = 0$ so au^{-1} is also nilpotent. Then $(1 - au^{-1})$ is a unit by the above calculation. Hence $u - a = u(1 - au^{-1})$ is a product of two units, and hence a unit. ◀

12. Define $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$, for all m, $n \in \mathbb{Z}$. Show that ϕ is an isomorphism of $\mathbb{Z}[\sqrt{2}]$ with itself.

▶ **Solution.** The mapping $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ given by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$, for all m, $n \in \mathbb{Z}$ is its own inverse since ϕ^2 is the identity. Therefore, ϕ is one-to-one and onto. Moreover,

$$\begin{aligned} \phi((m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2})) &= \phi((m_1 + m_2) + (n_1 + n_2)\sqrt{2}) \\ &= (m_1 + m_2) - (n_1 + n_2)\sqrt{2} \\ &= (m_1 - n_1\sqrt{2}) + (m_2 - n_2\sqrt{2}) \\ &= \phi(m_1 + n_1\sqrt{2}) + \phi(m_2 + n_2\sqrt{2}), \end{aligned}$$

and

$$\begin{aligned} \phi((m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2})) &= \phi((m_1m_2 + 2n_1n_2) + (m_1n_2 + m_2n_1)\sqrt{2}) \\ &= (m_1m_2 + 2n_1n_2) - (m_1n_2 + m_2n_1)\sqrt{2} \\ &= (m_1 - n_1\sqrt{2})(m_2 - n_2\sqrt{2}) \\ &= \phi(m_1 + n_1\sqrt{2})\phi(m_2 + n_2\sqrt{2}). \end{aligned}$$

It follows that ϕ is an isomorphism of $\mathbb{Z}[\sqrt{2}]$ with itself. ◀

13. What is the characteristic of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$?

► **Solution.** Since the order of $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m$ is the least common multiple of the order of a and the order of b, it follows that the order of the unit element $(1, 1)$ of $\mathbb{Z}_m \times \mathbb{Z}_n$ is the least common multiple of m and n, Thus, the characteristic of $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\text{lcm}(m, n)$. ◄

14. Let $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ be defined by $\phi(n + mi) = [n + 2m]_5$.

    (a) Show that ϕ is a ring homomorphism.

    ► **Solution.** The addition is easy to check. I will only check the multiplicative property:

$$\begin{aligned}
\phi((n + mi)(n' + m'i)) &= \phi((nn' - mm') + (mn' + nm')i) \\
&= [(nn' - mm') + 2(mn' + nm')]_5 \\
&= [(nn' + 4mm') + 2(mn' + nm')]_5 \\
&= [n + 2m]_5[n' + 2m']_5 \\
&= \phi(n + mi)\phi(n' + m'i).
\end{aligned}$$

    Thus, ϕ is a ring homomorphism. ◄

    (b) What is $\text{Ker}(\phi)$?

$$\begin{aligned}
\text{Ker}(\phi) &= \{n + mi \mid [n + 2m]_5 = [0]_5\} \\
&= \{n + mi \mid 5|(n + 2m)\}.
\end{aligned}$$

15. In the ring $\mathbb{Z}[i]$ of Gaussian integers (see Example 5.1.5) let $\langle p\rangle$ be the ideal generated by a prime number. Show that $\mathbb{Z}[i]/\langle p\rangle$ has p^2 elements, and has characteristic p.

    ► **Solution.** Since $p \cdot 1 \in \langle p\rangle$, it follows that $p \cdot (1 + \langle p\rangle) = p \cdot 1 + \langle p\rangle = 0 + \langle p\rangle$ so that 1 has additive order p in $\mathbb{Z}[i]/\langle p\rangle$. Thus the characteristic of this ring is p.

    Let $n_1 + n_2 i \in \mathbb{Z}[i]$. Using the division algorithm (for integers) write $n_1 = q_1 p + r_1$ and $n_2 = q_2 p + r_2$ where $0 \leq r_1, r_2 < p$. Then $(n_1 + n_2 i) + \langle p\rangle = (r_1 + r_2 i) + \langle p\rangle$ since $\langle p\rangle = \{m + ni \mid p|m \text{ and } p|n\}$. Thus, $\langle p\rangle$ has exactly p^2 cosets. This can also be shown by noting that the additive abelian group of $\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, while that of $\mathbb{Z}[i]/\langle p\rangle$ is $\mathbb{Z}_p \times \mathbb{Z}_p$. ◄

16. In the ring of Gaussian integers show that the ideal $\langle 5 - i\rangle$ is not a prime ideal.

    Hint: Show that $\mathbb{Z}[i]/\langle 5 - i\rangle \cong \mathbb{Z}_{26}$ by defining an onto ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[pi]/\langle 5 - i\rangle$ by $\phi(n) = n + \langle 5 - i\rangle$.

    ► **Solution.** Define $\phi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 5 - i\rangle$ by $\phi(n) = n + \langle 5 - i\rangle$, for all $n \in \mathbb{Z}$. This is the composition of the inclusion mapping from the subring $\mathbb{Z}$ into $\mathbb{Z}[i]$ and the natural projection mapping from $\mathbb{Z}[i]$ onto $\mathbb{Z}[i]/\langle 5 - i\rangle$ so it is the composition of two ring homomorphisms, and hence a ring homomorphism.

To show that ϕ is onto we will show that every coset of $\langle 5-i\rangle$ has an integer representative. To see this, note that $(a+5b)-(a+bi)=b(5-i)\in\langle 5-i\rangle$ so that

$$a+5b+\langle 5-i\rangle = a+bi+\langle 5-i\rangle.$$

Hence $\phi(a+5b)=a+5b+\langle 5-i\rangle = a+bi+\langle 5-i\rangle$ and since $a+bi$ is an arbitrary element of $\mathbb{Z}[i]$ it follows that ϕ is onto.

To determine $\ker(\phi)$, note that $26=(5+i)(5-i)\in\langle 5-i\rangle$. It follows that $26\in\ker(\phi)$ and hence $26\mathbb{Z}\subseteq\ker(\phi)$. To show the reverse inclusion, suppose that $n\in\ker(\phi)$. Then $n\in\langle 5-i\rangle$, so $n=c+di)(5-i)$ for some c, $d\in\mathbb{Z}$. Thus $n=5c+d$ and $5d-c=0$, so $c=5d$ and thus $n=26d\in 26\mathbb{Z}$.

It follows that $\mathbb{Z}[i]/\langle 5-i\rangle\cong\mathbb{Z}/26\mathbb{Z}$. Since $\mathbb{Z}/26\mathbb{Z}$ is not an integral domain, the ideal $\langle 5-i\rangle$ is not a prime ideal. ◀