I. Review homework problems.

II. Review quizzes.

III. Be able to prove short and straightforward theorems (e.g. see Problems 4 and 8 below).

Some practice problems for review

1. Which of the following functions are isomorphisms, which are homomorphisms of rings, and which are neither?

   (a) $f : \mathbb{Z} \to \mathbb{Z}$, defined by $f(n) = 3n$.
   Solution: $f : \mathbb{Z} \to \mathbb{Z}$ is not a homomorphism since $f(1 \cdot 2) = f(2) = 6$, while $f(1) \cdot f(2) = 18$, thus f does not preserve multiplication as there exist elements in $\mathbb{Z}$ such that $f(ab) \neq f(a)f(b)$.

   (b) $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, defined by $f(n) = 3n$.
   Solution: Let $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ is a homomorphism since for any $a, b \in \mathbb{Z}_6$ $f(a + b) = 3(a + b) = 3a + 3b = f(a) + f(b)$. Also, for any $a, b \in \mathbb{Z}_6$ $f(ab) = 3(ab)$. On the other hand, $f(a)f(b) = (3a)(3b) = 9ab = 3ab$. Note that in $\mathbb{Z}_6$, $3 = 9$. This homomorphism is not an isomorphism, since f is not injective: $f(0) = f(2) = 0$.

   (c) $g : \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\} \to \mathbb{R}$, defined by $g\left(\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \right) = x$.

   (d) $H : \mathbb{Q}[x] \to \mathbb{Q}[x]$, defined by $H(f(x)) = f^2(x)$.

   (e) $S : \mathbb{Z}_3[x] \to \mathbb{Z}_3[x]$, defined by $S(f(x)) = f^3(x)$.

   (f) $D : \mathbb{R}[x] \to \mathbb{R}[x]$ is the derivative map.

2. Let $K = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$. Show that the function $f : K \to K$, defined by $f(a + b\sqrt{5}) = a - b\sqrt{5}$ is an isomorphism of rings.

3. If $f : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism, prove that f is the identity map.

   Solution: Let $f : \mathbb{Z} \to \mathbb{Z}$ be an isomorphism. Then $f(0) = 0$ and $f(1) = 1$. We are going to employ proof by induction. Assume that for some $k \in \mathbb{N}$, $f(k) = k$. Then $f(k+1) = f(k)+f(1) = k+1$, since f preserves addition. Thus, by the Principle of Mathematical Induction, $f(n) = n$ for all nonnegative integers n. It remains to show $f(m) = m$ for all negative integers. Let $m \in \mathbb{Z}$, $m < 0$. Then $-m \in \mathbb{N}$ and by what we showed above $f(m) = f(-(-m)) = -f(-m) = -(-m) = m$. Thus, $f(n) = n$ for all integers n, i.e., f is the identity map on $\mathbb{Z}$.

4. Let $f : A \to B$ be a homomorphism of rings. Define $C = \{f(a) : a \in A\}$. Prove that C is a subring of B.

   Solution: It suffices to show that C is closed under subtraction and multiplication. Let $x, y \in C$ be arbitrary. Then there exist $a, b \in A$ such that $f(a) = x$ and $f(b) = y$. Thus, $x - y = f(a) - f(b) = f(a-b)$, since f is a homomorphism. Thus, $x-y$ is the image of an element in A under f, which shows that $x - y \in C$. Similarly, $xy = f(a)f(b) = f(ab)$, since f is a homomorphism. Thus, xy is the image of an element in A under f, which shows that $xy \in C$. Thus, we can conclude that C is a subring of B.

5. Show that the first ring is not isomorphic to the second.

   (a) $\mathbb{Z}_3 \times \mathbb{Z}_6$ and $\mathbb{Z}_9$

   Solution: $|\mathbb{Z}_3 \times \mathbb{Z}_6| = 18$, while $|\mathbb{Z}_9|$, since the two sets have different cardinalities, there does not exist a bijection between them.

   (b) $\mathbb{Z}_3 \times \mathbb{Z}_6$ and $\mathbb{Z}_{18}$

   Solution: Assume, by way of contradiction, that there exists an isomorphism $f : \mathbb{Z}_3 \times \mathbb{Z}_6 \to \mathbb{Z}_{18}$. Then $f(([0]_3, [0]_6)) = [0]_{18}$ and $f(([1]_3, [1]_6)) = [1]_{18}$ since an isomorphism sends the additive and multiplicative identities of the domain into the additive and multiplicative identities of the range respectively. Also, since f preserves addition, $f(([2]_3, [2]_6)) = [2]_{18}$, $f(([3]_3, [3]_6)) = f(([0]_3, [3]_6)) = [3]_{18}$, ..., $f(([0]_3, [0]_6)) = f(([6]_3, [6]_6)) = [6]_{18}$, which is a contradiction since $[0]_{18} \neq [6]_{18}$.

   (c) $\mathbb{Z}_2[x]/(x^2)$ and $\mathbb{Z}_4$

   (d) $\mathbb{Z}$ and $\{2x : x \in \mathbb{Z}\}$

6. Let F be a field, $c \in F \setminus \{0\}$ and $f(x) \in F[x]$. Show that $f(x)$ and $f(x) + c$ are relatively prime.

7. Determine if $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}_2$.

   Solution: Yes, it is reducible - note that $(x^2+x+1)(x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x+x^2+x+1 = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1$.

8. Let F be a field and $f(x), g(x), p(x) \in F[x]$, with $p(x) \neq 0_F$. It is given that the relation on $F[x]$ defined by $f(x) \equiv g(x) \pmod{p(x)}$ is an equivalence relation, i.e., it satisfies reflexivity, symmetry and transitivity. Let $[f(x)]_p$ denote the equivalence class of $f(x)$.

   Assume $[f(x)]_p \cap [g(x)]_p \neq \emptyset$.

   (i) Prove that $f(x) \equiv g(x) \pmod{p(x)}$.

   (ii) Use the above to show that $[f(x)]_p \subseteq [g(x)]_p$.

9. List the elements in $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Is this a field? Why or why not?

   Solution: $\mathbb{Z}_2[x]/(x^2+x+1) = \{[0], [1], [x], [x+1]\}$. The ring $\mathbb{Z}_2[x]/(x^2+x+1)$ is a field since x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$.

10. List the elements in $\mathbb{Z}_3[x]/(x^2 + x)$. Is this a field? Why or why not?

    Solution: $\mathbb{Z}_3[x]/(x^2+x) = \{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2], \}$. The ring $\mathbb{Z}_3[x]/(x^2+x)$ is not a field since it is not an integral domain: $[x][x + 1] = [0]$, i.e., there are two nonzero elements whose product is zero.

11. Explain why $[x + 1]$ is a unit in $\mathbb{Z}_5[x]/(x^2 + 2)$ and find its inverse.

    Solution: Note that $p(x) = x^2 + 2$ is irreducible in $\mathbb{Z}_5$, since it is a quadratic polynomial that has no roots in $\mathbb{Z}_5$. Indeed $p(0) = 2$, $p(1) = 2$, $p(2) = 1$, $p(3) = 1$, $p(4) = 3$. Therefore, $\mathbb{Z}_5[x]/(x^2+2)$ is a field and thus every nonzero element is a unit. Now, in order to find the multiplicative inverse of $[x + 1]$, apply the Division Algorithm to $x^2 + 2$ as dividend and $x + 1$ as divisor. Note that

    $$x^2 + 2 = (x + 1)(x - 1) + 3,$$

    which in $\mathbb{Z}_5[x]$ is equivalent to

    $$2(x^2 + 2) + (x + 1)(2 - 2x) = 1.$$

    This implies that in $\mathbb{Z}_5[x]/(x^2 + 2)$

    $$[x + 1] \cdot [3x + 2] = [1],$$

    i.e., $[x + 1]^{-1} = [3x + 2]$.

12. Show that $\mathbb{Q}[x]/(x^2 - 5)$ is isomorphic to $K = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$. Show that $f(x) = x^2 - 5$ has a root in K.