MTH 310: HW 6

Instructor: Matthew Cha

Due: June 25, 2018

1. (**Hungerford 5.3.5**) Verify that $\mathbb{Q}(\sqrt{3}) := \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$. Then, show that $\mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Q}[x]/\langle x^2 - 3\rangle$.

   Solution. By definition, we have the set containment $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$.
   Let $a + b\sqrt{3}$, $c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. We have that

   $$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$$
   $$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + \sqrt{3}(ad + bc) \in \mathbb{Q}(\sqrt{3}).$$

   Thus, $\mathbb{Q}(\sqrt{3})$ is closed under addition and multiplication.
   We have that $0 = 0 + 0\sqrt{3} \in \mathbb{Q}_3$ and $-(a + b\sqrt{3}) = -a - b\sqrt{3} \in \mathbb{Q}$. Therefore, $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$ is a subring.
   We can write $\mathbb{Q}[x]/\langle p\rangle$ as the set of congruence class modulo $p(x) = x^2 - 3$. Since we know that each congruence class is determined by a distinct representative of degree strictly less then 2 we have

   $$\mathbb{Q}[x]/\langle p\rangle = \{[a + bx]_p : a + bx \in \mathbb{Q}[x]\}.$$

   Define the map $f : \mathbb{Q}[x]/\langle p\rangle \to \mathbb{Q}(\sqrt{3})$ by $f([a + bx]_p) = a + b\sqrt{3}$. We want to show that f is an isomorphism. Let $[a + bx]_p, [c + dx]_p \in \mathbb{Q}[x]/\langle p\rangle$. We have that

   $$\begin{aligned} f([a + bx]_p + [c + dx]_p) &= f([(a + c) + (b + d)x]_p) \\ &= (a + c) + (b + d)\sqrt{3} \\ &= (a + b\sqrt{3}) + (c + d\sqrt{3}) \\ &= f([a + bx]_p) + f([c + dx]_p). \end{aligned}$$

   Since $[x^2]_p = [3]_p$ in $\mathbb{Q}[x]/ < p >$ we have that

   $$\begin{aligned} f([a + bx]_p[c + dx]_p) &= f([ac + (ad + bc)x + bdx^2]_p) \\ &= f([(ac + 3bd) + (ad + bc)x]_p) \\ &= (ac + 3bd) + (ad + bc)\sqrt{x} \\ &= (a + b\sqrt{3})(c + d\sqrt{3}) \\ &= f([a + bx]_p)f([c + dx]_p). \end{aligned}$$

   Thus, f respects addition and multiplication and is a homomorphism of rings.
   Let $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ be a general element. Then, f is surjective since $f([a + 3x]_p) = a + b\sqrt{3}$.
   Let $[a + bx]_p, [c + dx]_p \in \mathbb{Q}[x]/\langle p\rangle$ and suppose $f([a + bx]_p) = f([c + dx]_p)$. Then, $a + b\sqrt{3} = c + d\sqrt{3}$ and by basic arithmetic

   $$a - c = (b - d)\sqrt{3}.$$

   We know that $\sqrt{3}$ is not a rational number. If $b - d \neq 0$ then since $\mathbb{Q}$ is a field $b - d$ must be a unit. We could write $\sqrt{3} = \frac{a-c}{b-d} \in \mathbb{Q}$ which is a contradiction. Thus, $b = d$ and $a = c$. Equating coefficients we have that $a + bx = c + dx$ and thus $[a + bx]_p = [c + dx]_p$. Therefore, f is injective.

   We have proven that f is an isomorphism.

2. **(Hungerford 5.3.9)** Show that $\mathbb{Z}_2/\langle x^3+x+1\rangle$ is a field and contains all three roots of x^3+x+1.

   Solution. We know that $\mathbb{Z}_2$ is a field since 2 is prime.

   Let $p(x) = x^3+x+1$ in $\mathbb{Z}_2[x]$. Since $p(0) = 1$ and $p(1) = 1^3+1+1 = 1$ in $\mathbb{Z}_2[x]$ we conclude by the Factor Theorem that p has no roots in $f(x)$. p is degree 3 and has no roots, thus p is irreducible. Therefore, $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ is a field.

   Since $\mathbb{Z}_2 \subset \mathbb{Z}_2[x]/\langle p\rangle$ is a field extension, we can think of $p(x) = x^3+x+1$ as a polynomial with coefficients in the field $\mathbb{Z}_2[x]/\langle p\rangle$. By the Factor Theorem and its Corollary 4.17, since $p(x) = x^3+x+1$ is a degree 3 polynomial it can have at most 3 distinct roots in $\mathbb{Z}_2[x]/\langle p\rangle$.

   Let's check that $\{[x]_p, [x^2]_p, [x^2+x]_p\}$ are the three distinct roots. We will use the simple relations $[x+1]^2 = [x^2+1]$, $[x^3+x+1]_p = [0]_p$, and $[x^3]_p = [x+1]_p$. Thus we have that

$$
\begin{aligned}
p([x]_p) &= [x]_p^3 + [x]_p + [1]_p \\
&= [x^3+x+1]_p \\
&= [0]_p \\
p([x^2]_p) &= [x^2]_p^3 + [x^2]_p + [1]_p \\
&= [x^3]_p^2 + [x^2]_p + [1]_p \\
&= [x+1]_p^2 + [x^2]_p + [1]_p \\
&= [x^2+1]_p + [x^2+1]_p \\
&= [0]_p \\
p([x^2+x]_p) &= [x^2+x]_p^3 + [x^2+x]_p + [1]_p \\
&= [x^3(x+1)^3]_p = [x^2+x+1]_p \\
&= [(x+1)^4]_p + [x^2+x+1]_p \\
&= [(x^2+1)(x^2+1)]_p + [x^2+x+1]_p \\
&= [x^4+1]_p + [x^2+x+1]_p \\
&= [(x+1)x+1]_p + [x^2+x+1]_p \\
&= [x^2+x+1]_p + [x^2+x+1]_p \\
&= [0]_p.
\end{aligned}
$$

3. **(Hungerford 6.1.6)** Show that the set of nonunits in $\mathbb{Z}_8$ is an ideal.

   Solution.

   Recall that in a past HW we showed that $[a] \in \mathbb{Z}_8$ is either a unit or zero divisor, and $[a]$ is a zero-divisor if and only if the gcd of $(a, 8) > 1$. Thus, $I = \{[a] \in \mathbb{Z}_8 : [a] \text{ is a zero divisor}\} = \{[a] \in \mathbb{Z}_8 : (a, 8) > 1\}$. We need to show that I is a subring and satisfies the ideal property.

   (subring) Let $[a], [b] \in I$ and define the gcds $d_1 = (a, 8) > 1$ and $d_2 = (b, 8) > 1$. It follows that d_1, d_2 must be either 2 or 4 since these are the only proper divisors of 8. Thus, $2|d_1$ and $2|d_2 \implies 2|a$ and $2|b \implies 2|a+b$ and $2|ab$. We have shown that the gcd of $(a+b, 8) \geq 2$ and $(ab, 8) \geq 2$ so that $a+b$ and ab are a zero-divisors in $\mathbb{Z}_8$. Therefore, $[a]+[b] \in I$ and $[a][b] \in I$.

   By definition $[0]$ is a zero-divisor $\implies [0] \in I$. Since a and $-a$ have the same set of divisors this implies that the gcd $(-a, 8) = (a, 8) > 1$. Thus, $[-a] \in I$.

   Therefore by the subring theorem I is a subring.

   (ideal property) Let $[a] \in I$ and $[r] \in \mathbb{Z}_8$. Let $d = (a, 8) > 1$ be the gcd. Then, $d|a \implies d|ra$. Thus, $(ra, 8) \geq (a, 8) > 1$. Therefore $[r][a] \in I$. Since $\mathbb{Z}_8$ is commutative, we conclude that I satisfies the ideal property.

4. **(Hungerford 6.1.23)** Verify that $I = \{0, 3, 6, 9, 12\}$ is an ideal in $\mathbb{Z}_{15}$ and list all distinct cosets.

   Solution. Notice that we have the following set inclusions

$$I = \{[r] : 0 \leq r < 15 \text{ and } 3|r\} \subset \{[3k] : k \in \mathbb{Z}\}.$$

Using the division algorithm, we can write $3k = 15q + r$ for some $0 \leq r < 15$. It follows that $r = 3(k - 5q)$ so that $3|r$. Therefore we have shown that

$$I = \{[3k] : k \in \mathbb{Z}\}.$$

We need to show that I is a subring and has the ideal property.

(subring) Let $[3k], [3j] \in I$. We have that $[3k] + [3j] = [3(k + j)] \in I$ and $[3k][3j] = [3(3kj)] \in I$. Thus I is closed under addition and multiplication.

If $k = 0$ then $[3k] = [3 \cdot 0] = [0] \in I$ and $-[3k] = [3(-k)] \in I$.

Therefore, by the subring theorem we have that I is a subring.

(ideal property) Let $[a] \in \mathbb{Z}_{15}$ and $[3k] \in I$. Then, $[a][3k] = [3(ak)] \in I$. Since $\mathbb{Z}_{15}$ is commutative, we conclude that I has the ideal property.

Therefore, I is an ideal.

The cosets of I are $\mathbb{Z}_{15}/\langle I\rangle = \{[a]+I : [a] \in \mathbb{Z}_{15}\}$. We have that $[a]+I = [b]+I$ if and only if $[a-b] \in I$ if and only if $[a - b] = [3k]$ for some $k \in \mathbb{Z}$. Thus, $(a - b) - 3k = 15j \iff a - b = 3(5j + k)$, that is, $a \equiv b \mod 3$. Therefore, distinct cosets are equal if and only if their remainder modulo 3 are equal. We conclude that there are three distinct cosets

$$\mathbb{Z}_{15}/\langle I\rangle = \{[0] + I, [1] + I, [2] + I\}.$$

5. **(Hungerford 6.1.35)** Let $I \subset \mathbb{Z}$ be an ideal such that $\langle 3\rangle \subset I \subset \mathbb{Z}$. Prove that either $I = \langle 3\rangle$ or $I = \mathbb{Z}$.

   Solution. If $I = \langle 3\rangle$ then we are done.

   Suppose $I \neq \langle 3\rangle$ and let $a \in I$ be such that $a \notin \langle 3\rangle$. Since 3 is prime and 3 does not divide a we have that the gcd of $(3, a) = 1$. It follows that there are $u, v \in \mathbb{Z}$ such that $3u + av = 1$. Moreover, $av \in i$ and si nce $3 \in \langle 3\rangle$ we have that $3 \in I$ and $3u \in I$. I is a subring so $1 = 3u + av \in I$.

   For any $a \in \mathbb{Z}$ we have that $a = a \cdot 1 \in I$. Therefore $I = \mathbb{Z}$.

6. Let $a \in \mathbb{R}$ and consider the evaluation homomorphism $\phi : \mathbb{R}[x] \to \mathbb{R}$ where $\phi(f(x)) = f(a)$. Find the kernel of ϕ.

   Solution. By definition $\ker\phi = \{f(x) \in \mathbb{R}[x] : \phi(f(x)) = 0\}$. Thus, $f(x) \in \ker\phi$ if and only if $\phi(f(x)) = 0$ if and only if $f(a) = 0$. Since $\mathbb{R}$ is a field we can apply the Factor Theorem to see that $f(x) \in \ker\phi$ if and only if $x - a|f(x)$, that is $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$. We conclude that the kernel of ϕ is the principal ideal generated by $x - a$

$$\ker\phi = \langle x - a\rangle$$

7. **(Hungerford 6.2.12)** Let I be an ideal in a noncommutative ring R such that $ab - ba \in I$ for all $a, b \in R$. Prove that R/I is commutative.

   Solution.

   By assumption $ab - ba \in I$ for all $a, b \in R$. It follows that $(ab - ba) + I = 0_R + I$ for all $a, b \in R$.

   Let $a + I, b + I \in R/I$ be arbitrary cosets of I. We have that

$$\begin{aligned}(a + I)(b + I) - (b + I)(a + I) &= ((ab) + I) - ((ba) + I)\\ &= (ab - ba) + I\\ &= 0_R + I.\end{aligned}$$

   By definition, R/I is commutative.

8. **(Hungerford 6.2.21)** Use the First Isomorphism Theorem to show that $\mathbb{Z}_{20}/\langle[5]\rangle$ is isomorphic to $\mathbb{Z}_5$.

Solution. Define the function $f : \mathbb{Z}_{20} \to \mathbb{Z}_5$ by $f([a]_{20}) = [a]_5$.

(well-defined) Since we define the function by its action on representatives, first we must show the function is well defined. Suppose $[a]_2 0 = [b]_2 0$. Thats, if and only if $a - b = 20k = 5(4k)$ for some $k \in \mathbb{Z}$ if and only if $f([a]_{20}) = [a]_5 = [b]_5 = f([b]_{20})$. Thus, f is well defined.

(surjective) Let $[a]_5 \in \mathbb{Z}_5$. Then, $f([a]_{20}) = [a]_5$ thus f is surjective.

(homomorphism) Let $[a]_{20}, [b]_{20} \in \mathbb{Z}_{20}$. Then,

$$\begin{aligned} f([a]_{20} + [b]_{20}) &= f([a+b]_{20}) \\ &= [a+b]_5 \\ &= [a]_5 + [b]_5 \\ &= f([a]_{20}) + f([b]_{20}), f([a]_{20}[b]_{20}) && = f([ab]_{20}) \\ &= [ab]_5 \\ &= [a]_5[b]_5 \\ &= f([a]_{20})f([b]_{20}). \end{aligned}$$

Therefore f is a homomorphism of rings.

(kernel) We claim that $\ker f = \langle[5]_{20}\rangle$. Notice that $f([5]_{20}) = [5]_5 = [0]_5 \implies [5]_{20} \in \ker f$. Since f is a homomorphism $f([a]_{20}[5]_{20}) = [a]_5[0]_5 = [0]_5 \implies \langle[5]_{20}\rangle \subset \ker f$. Let $[a]_{20} \in \ker f$. Then $f([a]_{20}) = [a]_5 = [0]_5$. Thus we have that $5|a$ if and only if $a = 5b$ for some $b \in \mathbb{Z}$ if and only if $[a]_{20} = [5b]_{20} = [5]_{20}[b]_{20} \in \langle[5]_{20}\rangle$. Therefore, $\ker f = \langle[5]_{20}\rangle$.

By the First Isomorphism Theorem, the map $\phi : \mathbb{Z}_{20}/\langle[5]_{20}\rangle \to \mathbb{Z}_5$ defined by $\phi(a + \langle 5\rangle) = f(a)$ is an isomorphism.

9. **(Hungerford 6.3.5)** List all maximal ideals in $\mathbb{Z}_6$. Do the same in $\mathbb{Z}_{12}$.

Solution. Let I be an ideal of $\mathbb{Z}_6$.

If I contains a unit, $a \in I$ then $aa^{-1} = [1] \in I$. Thus, for any $[b] \in \mathbb{Z}_6$ we have that $[b] = [b][1] \in I$. Therefore $I = \mathbb{Z}_6$.

If $I \neq \mathbb{Z}_6$ then $I \subset \{[0], [2], [3], [4]\}$ the set of non-units in $\mathbb{Z}_6$. Note that I must be a strict subset since if $[2], [3] \in I$ then $[3] - [2] = [1] \in I$ which would imply that $I = \mathbb{Z}_6$. We know that $[0] \in I$. We can check by hand that the following subsets are principal ideals:

$$\begin{aligned} \{[0]\} \\ \{[0], [2], [4]\} = \langle[2]\rangle = \langle[4]\rangle \\ \{[0], [3]\} = \langle[3]\rangle \end{aligned}$$

Moreover, the subset $\{[0], [2]\}$, $\{[0], [4]\}$, $\{[0], [3], [4]\}$, $\{[0], [2], [3]\}$ are not ideals. Therefore, $\mathbb{Z}_6$ has a total of 2 non-trivial ideals $\{[0], [2], [4]\}$ and $\{[0], [3]\}$. They are both maximal.

10. **(Hungerford 6.3.13)**

   (a) Let $I \subset R$ be an ideal. Prove that $I \times I$ is an ideal in $R \times R$.

   (b) Prove that $(R \times R)/(I \times I)$ is isomorphic to $R/I \times R/I$. (*Hint*: Consider the function $f((a, b)) = (a + I, b + I)$.)

Solution.

(a) Since $I \times I \subset R \times R$ are both rings this implies that $I \times I$ is a subring.

We must show the ideal property holds. Let $(a, b) \in R \times R$ and $(i, j) \in I \times I$. Then, $ai \in I$ and $bj \in I$ since I is an ideal. Therefore, $(ai, bj) \in I \times I$.

(b) Define the function $f : R \times R \to R/I \times R/I$ by $f((a,b)) = (a+I, b+I)$. Then, by its definition f is surjective.

Let $(a,b),(c,d) \in R \times R$. We have that

$$\begin{aligned} f((a,b)+(c,d)) &= f((a+c,b+d)) \\ &= ((a+c)+I,(b+d)+I) \\ &= (a+I,b+I)+(c+I,d+I) \\ &= f((a,b))f((c,d)), \\ f((a,b)\cdot(c,d)) &= f((ac,bd)) \\ &= ((ac)+I,(bd)+I) \\ &= (a+I,b+I)\cdot(c+I,d+I) \\ &= f((a,b))f((c,d)). \end{aligned}$$

Therefore f is a homomorphism.

The following statement follows directly: $i \times j \in I \times I$ if and only if $i+I = j+I = 0_R + I$. if and only if $f((i,j)) = (i+I, j+I) = (0_R + I, 0_R + I)$. Therefore, $\ker f = I \times I$.

By the First Isomorphism Theorem, we conclude that $R \times R/(I \times I) \cong R/I \times R/I$.