MATH 403 Winter 2018
Homework II
Winter 2018

Problem 2.1 (PS 1,4.1 in 403A): Judson 16.6.1

1. Depending whether you accept a ring to have a multiplication identity or not, your answer will be yes if you allowed rings to have no multiplicative idenity. This is not a field because 7 does not have a mupltiplicative inverse.

2. Show that if $a = a'$ mod 18 and $b = b'$ mod 18, then $ab = a'b'$ mod 18. This is a ring but not a field becaue it is not an integral domain. For example, $6 \cdot 3 = 0$.

3. Note that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Hence
$$(a + b\sqrt{2})(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \cdot \sqrt{2}) = 1.$$
Obviously $a^2 - 2b^2 \in \mathbf{Q}$ hence $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2} \cdot \sqrt{2} \in \mathbf{Q}(\sqrt{2})$ is the inverse.

4. Note that
$$\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2})(\sqrt{3}).$$
Similarly, for all $a, b \in \mathbf{Q}(\sqrt{2})$ we have
$$(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2.$$
Then we already proved $\mathbf{Q}(\sqrt{2})$ is a field so that $\frac{a}{a^2-3b^2}, \frac{b}{a^2-3b^2}$ are also in $\mathbf{Q}(\sqrt{2})$. Then
$$\frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2} \cdot \sqrt{3}$$
is the inverse for $a + b\sqrt{3}$.

5. This is a ring but not a field. Consider $\sqrt{3}$. If $1/\sqrt{3} \in \mathbf{Z}(\sqrt{3})$, then there are $a, b \in \mathbf{Z}$ such that $a + b\sqrt{3} = 1\sqrt{3}$. Then $a\sqrt{3} + 3b = 1$ so that $a\sqrt{3} = 1 - 3b \in \mathbf{Z}$. This implies $\sqrt{3} \in \mathbf{Q}$.

6. This is not a ring.

7. This is a ring but not a field. You will compute the units later.

8. This ring is a vector space over $\mathbf{Q}$ with spanning set $\{1, 3^{1/3}, 3^{2/3}\}$. Hence it is finite dimensional (less than 3). For a non-zero element $\alpha \in \mathbf{Q}(3^{1/3})$, the set $\{1, \alpha, \alpha^2, \alpha^3\}$ has to be linearly dependent over $\mathbf{Q}$. Then α is zero of a non-zero polynomial $f \in \mathbf{Q}[x]$. Among all polynomials havinfg α as a root, take an f that has the smallest degree. Then I claim that f has nonzero constant term. If not, then $f = xf'$ and
$$0 = f(\alpha) = \alpha \times f'(\alpha) \in \mathbf{Q}(3^{1/3}) \subset \mathbf{R}$$
. Since $\alpha \neq 0$, and $\mathbf{R}$ is a field, we have $f'(\alpha) = 0$, contradicting the assumption that f is of the smallest degree. Now write $f(x) = a_n x^n + \cdots c_0$, then
$$0 \neq c_0 = x(-a_n x^{n-1} - \cdots - a_1).$$
Plugging in α, we see that α has a multiplicative inverse.

PS $\sharp$4.3 in 403A (Problem 2.3)

1. Prove that the set $R^\times$ of units of a ring R is a group under multiplication. Then $R^\times$ has t elements. The order of an element in a finite group necessarily divides of size of the group. Hence $u^t = 1$ for all $u \in R^\times$.

2. $(\mathbf{Z}/n)^\times$ are represented by integers that are relative prime to n. $\varphi(n)$ is then the size of $(\mathbf{Z}/n)^\times$. Now apply (a).

Problem 2.4 (PS ♯5.1 in 403A): Goodman 1.11.9

For a, let $\pi_a : \mathbf{Z} \to \mathbf{Z}/a$ be the quotient map, which is a ring homomorphism. Let $\pi_b : \mathbf{Z} \to \mathbf{Z}/b$ be the quotient map for b. Then this induces a map $\pi : \mathbf{Z} \to \mathbf{Z}/a \oplus \mathbf{Z}/b$. The kernel of this map is the integers that are divisible by both a and b. Since $(a, b) = 1$, the kernel of π is the ideal generated by $a \cdot b$. Then π factors through $\pi_{a,b} : \mathbf{Z}/ab \to (\mathbf{Z}/a) \oplus (\mathbf{Z}/b)$.

PS ♯5.5 in 403A (Problem 2.8 Judson 16.6.7)

Suppose there is an isomorphism $\varphi : \mathbf{C} \to \mathbf{R}$ of rings. Then $\varphi(1) = 1$ so $\varphi(-1) = -1$. Let $\varphi(i) = \alpha \in \mathbf{R}$ Then

$$-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2 = \alpha^2.$$

There is no real number α that can satisfy $\alpha^2 = -1$. Hence $\mathbf{C}$ is not isomorphic to $\mathbf{R}$ as rings.

Problem 2.11 (PS ♯6.3 in 403A): Judson 16.6.11

Simply note that $\mathbf{Z}[i]$ is a subring of $\mathbf{C}$, which is an integral domain.

PS ♯6.4 in 403A (Problem 2.12)

The norm $|| \cdot || : \mathbf{C} \to \mathbf{R}$ on $\mathbf{C}$ is multiplicative. Henec if $a + bi$ has a unit in $\mathbf{Z}[i]$ and $c + di$ is its inverse, we have $(a^2 + b^2)(c^2 + d^2) = 1$. The only integers (a, b) that satisifies this are $(0, \pm 1)$, $(\pm 1, 0)$. They corresponds to ± 1 and $\pm i$. One checks that they are indeed units.