Solutions to Homework #17

1. Saracino, Section 16, Problem 16.3:
Let $F = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$. Prove that F is a field under ordinary addition and multiplication.

Proof. We have $0 + 0\sqrt{2} \in F$, so F is nonempty.
Given $x, y \in F$, write $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ with $a, b, c, d \in \mathbb{Q}$. Then

$$x - y = (a + b) - (c + d)\sqrt{2} \in F \quad \text{and} \quad xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in F,$$

so that $F \subseteq \mathbb{R}$ is indeed closed under both $-$ and $\cdot$. By Corollary 17.2, then, F is a subring of $\mathbb{R}$.

Note also that $\cdot$ is commutative on $\mathbb{R}$, since for any $x, y \in F$, we have $x, y \in \mathbb{R}$, and hence $x \cdot y = y \cdot x$. In addition, $1 = 1 + 0\sqrt{2} \in F$, so for any $x \in F$, we have $x \in \mathbb{R}$, and hence $x \cdot 1 = 1 \cdot x = x$. Thus, F is a commutative ring with unity. It remains only to show that every element of $F \smallsetminus \{0\}$ has a multiplicative inverse in F.

Given $x = a + b\sqrt{2} \in F \smallsetminus \{0\}$, we have $a, b \in \mathbb{Q}$, not both zero. Then $a^2 \neq 2b^2$, as otherwise we would either have $(a/b)^2 = 2$ (so that $\sqrt{2} \in \mathbb{Q}$, a contradiction) or else $b = 0$ and hence $a = 0$ (also a contradiction, to our assumption that a and b are not both 0). Hence we have $a^2 - 2b^2 \neq 0$. Let

$$y = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2} \in F.$$

Then

$$yx = xy = \frac{a^2 - 2b^2}{a^2 - 2b^2} + \frac{ba - ab}{a^2 - 2b^2}\sqrt{2} = 1,$$

as desired. QED

---

2. Saracino, Section 16, Problem 16.7: Let F be a field, let $a, b \in F$, and assume $a \neq 0$. Show that the equation $ax + b = 0$ can be solved for $x \in F$; that is, there exists $x \in F$ that makes the equation true.

Proof. We have $a^{-1} \in F$, since F is a field and $a \in F \smallsetminus \{0\}$. Let $x = -a^{-1}b \in F$. Then

$$ax + b = a(-a^{-1}b) + b = -\big(aa^{-1}b\big) + b = -(1b) + b = -b + b = 0,$$

where the second equality is by Theorem 16.1(ii). QED

---

3. Saracino, Section 16, Problem 16.18, slight variant:
Let R be a nontrivial ring with unity (so $1 \neq 0$), and assume that R has no nonzero zero-divisors. Let $a, b \in R$ with $ab = 1$. Prove that $ba = 1$ also.

Proof. Given $a, b \in R$ with $ab = 1$, we first claim that $a \neq 0$. Indeed, if $a = 0$, then $1 = ab = 0b = 0$, contradicting the fact that $1 \neq 0$ and proving our claim.
Next, observe that

$$a(ba - 1) = a(ba) - a1 = (ab)a - a = 1a - a = a - a = 0.$$

Since $a \neq 0$, this shows that $ba - 1$ is a zero-divisor. Since R has no nonzero zero-divisors, then, we have $ba - 1 = 0$. That is, $ba = 1$. QED

Note: I allowed you to assume $1 \neq 0$, but Saracino doesn't restrict to that case. That's because the result is (trivially) true even if $1 = 0$. In that case, we get that $R = \{0\}$ is trivial, by Corollary 16.2. Then for any $a, b \in R$, we have $ba = 0 = 1$.

---

4. Saracino, Section 16, Problem 16.24, variant:
Let $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$. For any $r = a + bi \in \mathbb{Z}[i]$, define the *norm* $N(r)$ by $N(r) = a^2 + b^2$.

(a) Prove that for all $r, s \in \mathbb{Z}[i]$, we have $N(rs) = N(r)N(s)$.

(b) Show that $r \in \mathbb{Z}[i]$ is a unit if and only if $N(r) = 1$.

(c) Use part (b) to find all the units in $\mathbb{Z}[i]$. (And (briefly) justify your answer, of course.)

Proof. (a): Given $r, s \in \mathbb{Z}[i]$, write $r = a + bi$ and $s = c + di$ with $a, b, c, d \in \mathbb{Z}$. Then

$$N(rs) = N\big((ac-bd)+(ad+bc)i\big) = (ac-bd)^2+(ad+bc)^2 = (a^2c^2-2abcd+b^2d^2)+(a^2d^2+2abcd+b^2c^2)$$
$$= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (a^2+b^2)(c^2+d^2) = N(r)N(s).$$

(b): Given $r \in \mathbb{Z}[i]$, we must show the "iff" statement.

($\Rightarrow$): Since r is a unit, there is some $s \in \mathbb{Z}[i]$ such that $rs = 1$. By part (a), then,

$$N(r)N(s) = N(rs) = N(1) = 1^2 + 0^2 = 1.$$

However, both $N(r)$ and $N(s)$ are nonnegative integers. The only way the product of two nonnegative integers can be 1 is for both multiplicands to be 1. Thus, $N(r) = 1$.

($\Leftarrow$): Write $r = a + bi$ with $a, b \in \mathbb{Z}$; we are assuming $a^2 + b^2 = N(r) = 1$.

Let $s = a - bi \in \mathbb{Z}[i]$. Then $sr = rs = (a + bi)(a - bi) = a^2 + b^2 = 1$. Thus, r has multiplicative inverse $s \in \mathbb{Z}[i]$ and hence is a unit. QED

(c): We claim the set of units in $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$. Indeed, each of these four elements is a unit, since $N(\pm 1 + 0i) = 1 = N(0 + (\pm 1)i)$. Conversely, if $a + bi \in \mathbb{Z}[i]$ is a unit, then $a^2 + b^2 = 1$, and hence either $a^2 = 1$ and $b^2 = 0$ or $a^2 = 0$ and $b^2 = 1$. In the former case, $a + bi = \pm 1$, and in the latter case, $a + bi = \pm i$, proving our claim. QED

---

5. Saracino, Section 17, Problem 17.2(a,c), ideals only:

Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$ be the ring of real-valued functions on the real line, under ordinary addition and multiplication of functions. Which of the following subsets S of R are ideals?

[As always, prove your answers.]

(a) $S = \{f \in R \,|\, f(1) = 0\}$

(c) $S = \{f \in R \,|\, f(3) = f(4)\}$

Solution. (a): YES, ideal

(Nonempty): The zero-function $0_R(x) = 0$ has $0_R \in R$ with $0_R(1) = 0$, so $0_R \in S$.

(Closed): Given $f, g \in S$, we have $(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$, so $f - g \in S$.

(Sticky): Given $f \in S$ and $h \in R$, we have $fh = hf$, and $(fh)(1) = f(1) \cdot h(1) = 0 \cdot h(1) = 0$, so $hf = fh \in S$. QED (a)

(c): NO, not ideal

Let $f(x) = 1$, and let $g(x) = x$, so that $f, g \in R$. Note also that $f(3) = 1 = f(4)$, so $f \in S$. However, $fg = g$ is **not** in S, because $g(3) = 3 \neq 4 = g(4)$. Thus, S does not satisfy the sticky property. QED

---

6. Saracino, Section 17, Problem 17.25(a):

Let R be a ring, and let I and J be ideals of R. Prove that $I \cap J$ is an ideal of R.

Proof. (**Nonempty**): We have $0_R \in I$ and $0_R \in J$, since they are both ideals. Thus, $0_R \in I \cap J$.

(**Closed**): Given $x, y \in I \cap J$, then $x - y \in I$ since $x, y \in I$ and I is an ideal. Similarly, $x - y \in J$. Thus, $x - y \in I \cap J$.

(**Sticky**): Given $x \in I \cap J$ and $r \in R$, we have $x \in I$, and hence $xr, rx \in I$, since I is an ideal. Similarly, $xr, rx \in J$. Thus, $xr, rx \in I \cap J$. QED