HW1 SOLUTION

JI ZENG

Only problems with provided solutions will be graded. Solutions might be concise for some problems, but please be noticed that they don't reflect the wanted level of detailedness of your answer.

Armstrong.2.8
By definition of inverse, we need to check $(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = e$, where e means the identity.
Indeed,

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= xyy^{-1}x^{-1} = x(yy^{-1})x^{-1} \\ &= x(e)x^{-1} = xx^{-1} = e,\end{aligned}$$

as wanted. And similarly $(y^{-1}x^{-1})(xy) = e$.

Armstrong.3.2
Notice that if $a - b\sqrt{2} = 0$, then $a = b = 0$, hence $a + b\sqrt{2} = 0$. So provided $a + b\sqrt{2} \neq 0$, we have $a - b\sqrt{2} \neq 0$. So we have the following computation

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2}.\end{aligned}$$

This means we can express $\frac{1}{a+b\sqrt{2}} = c + d\sqrt{2}$ with $c = \frac{a}{a^2-2b^2}, d = \frac{-b}{a^2-2b^2} \in \mathbb{Q}$.
Now we check briefly that $G := \mathbb{Q}(\sqrt{2}) - \{0\}$ is a group with multiplication. Firstly we need to show that G is closed under multiplication. If $x = a+b\sqrt{2}, y = c+d\sqrt{2} \in G$ with $a, b, c, d \in \mathbb{Q}$, then

$$\begin{aligned}xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= (ac + 2bd) + (ad + bc)\sqrt{2},\end{aligned}$$

with $ac + 2bd, ad + bc \in \mathbb{Q}$. Also $xy \neq 0$ as in the common multiplication of real numbers. So $xy \in G$ as wanted.
Secondly the multiplication is associative as it's the well-known multiplication of real numbers. Also we have the identity $1 \in G$.
Finally, by the process above we know that for $a + b\sqrt{2} \in G$, $\frac{1}{a+b\sqrt{2}} \in G$, which means the inverse always exists.

Problem.A
(1) Suppose e_1 and e_2 are two neutral elts of G, then

$$e_1 = e_1 * e_2, \text{ because } e_2 \text{ is neutral}$$

$$= e_2, \text{ because } e_1 \text{ is neutral.}$$

Hence $e_1 = e_2$, which means there's at most one neutral elt.
(2) An empirical example: the positive integers under addition.
A trivial example: $G = \{a, b\}$ with multiplication defined to be

$$a * a = a * b = b * a = b * b := a.$$

Or other example you come up with.

Problem.B
(1) Suppose b_1 and b_2 are two inverses of a in G, then

$$\begin{aligned} b_1 = b_1 * e = b_1 * (a * b_2), &\text{ because } b_2 \text{ is a inverse of } a. \\ = (b_1 * a) * b_2 = e * b_2 = b_2, &\text{ by associative law and } b_1 \text{ being a inverse of } a. \end{aligned}$$

Hence $b_1 = b_2$.
(2) The neutral elt in $\mathbb{Z}$ with multiplication is 1. Elements with inverse are exactly those elts n s.t. $\frac{1}{n}$ is an integer. So they are $\{\pm 1\}$.

Problem.D
(a) We use Euclid algorithm:
$1147 = 1 \cdot 899 + 248$, so $gcd(1147, 899) = gcd(899, 248)$.
$899 = 3 \cdot 248 + 155$, so $gcd(899, 248) = gcd(248, 155)$.
$248 = 1 \cdot 155 + 93$, so $gcd(248, 155) = gcd(155, 93)$.
$155 = 1 \cdot 93 + 62$, so $gcd(155, 93) = gcd(93, 62)$.
$93 = 1 \cdot 62 + 31$, so $gcd(93, 62) = gcd(62, 31)$.
$62 = 2 \cdot 31$, so $gcd(62, 31) = 31$.
We use the fact $nm = lcm(n, m)gcd(n, m)$, we compute $lcm(1147, 899) = 33263$.
(b) We gather the number above

$$\begin{aligned} 31 &= 93 - 62 = 93 - (155 - 93) = 2 \cdot 93 - 155 \\ &= 2 \cdot (248 - 155) - 155 = 2 \cdot 248 - 3 \cdot 155 \\ &= 2 \cdot 248 - 3 \cdot (899 - 3 \cdot 248) = 11 \cdot 248 - 3 \cdot 899 \\ &= 11 \cdot (1147 - 899) - 3 \cdot 899 = 11 \cdot 1147 - 14 \cdot 899 \end{aligned}$$

(c) $1147 = 31 \cdot 37$ and $899 = 31 \cdot 29$.