ANSWERS TO SOME OF THE HOMEWORK PROBLEMS

Note: these answers are not proofread. Also, the style is somewhat more terse than I would want to see on a problem set or exam, but I hope this will give you an indication of various ways to think about some the the homework problems.

First problem set

1. (i) $\mathbb{Z}[\frac{1}{2}]$ is an additive subgroup: $a/2^n + b/2^m = (2^m a + 2^n b)/2^{n+m} \in \mathbb{Z}[\frac{1}{2}]$, $0 = 0/2^n$ for any $n \geq 0$ is in $\mathbb{Z}[\frac{1}{2}]$, and given $a/2^n \in \mathbb{Z}[\frac{1}{2}]$, $-(a/2^n) = (-a)/2^n \in \mathbb{Z}[\frac{1}{2}]$. Also, $\mathbb{Z}[\frac{1}{2}]$ is closed under multiplication as $a/2^n \cdot b/2^m = (ab)/2^{n+m} \in \mathbb{Z}[\frac{1}{2}]$. Finally $1 = 1/2^0 = 2/2 \in \mathbb{Z}[\frac{1}{2}]$. Clearly, if $a \in \mathbb{Z}$, $a/2^0 = a \in \mathbb{Z}[\frac{1}{2}]$, and similarly $1/2 \in \mathbb{Z}[\frac{1}{2}]$ as well.

(ii) S is an additive subgroup: $a_1/b_1 + a_2/b_2 = (a_1b_2 + a_2b_1)/(b_1b_2)$, and, if 2 does not divide b_1 or b_2, then 2 does not divide the product b_1b_2. Hence the sum is in S. Clearly $0 = 0/1 \in S$, and given $a/b \in S$, $-(a/b) = (-a)/b \in S$. Thus S is an additive subgroup. Also, S is closed under multiplication as $a_1/b_1 \cdot a_2/b_2 = (a_1a_2)/(b_1b_2)$, and as before if 2 does not divide b_1 or b_2, then 2 does not divide b_1b_2. Hence S is closed under multiplication. As before, $1 = 1/1$ and more generally, for $a \in \mathbb{Z}$, $a = a/1 \in S$. If $1/2 \in S$, then $1/2 = a/b$ where 2 does not divide b, and hence $b = 2a$ which is a contradiction.

2. A careful definition of r^n would be inductively: $r^0 = 1$ and, for all $n \geq 0$, $r^{n+1} = r^n r$. Then we can prove the statement $r^n r^m = r^{n+m}$ by induction on m, starting with the case $m = 0$ where it is just the statement that $r^n \cdot 1 = r^n$. Suppose it is true for m: for all $r \in R$ and for all $n \in \mathbb{N}$, $r^n r^m = r^{n+m}$. Then $r^n r^{m+1} = r^n r^m r$, by definition, and $r^n r^m r = r^{n+m} r$ by the inductive hypothesis. Again by definition, $r^{n+m} r = r^{n+m+1}$, completing the inductive step.
To see that $(r^n)^m = r^{nm}$, we again argue by induction on m starting with the case $m = 0$, where both sides are 1. Suppose that, for a given $m \in \mathbb{N}$ and all $r \in R$ and for all $n \in \mathbb{N}$, $(r^n)^m = r^{nm}$. Then $(r^n)^{m+1} = (r^n)^m r^n$, by the inductive definition given above. Then using the inductive hypothesis and the first part,

$$(r^n)^m r^n = r^{nm} r^n = r^{nm+n} = r^{n(m+1)},$$

hence $(r^n)^{m+1} = r^{n(m+1)}$, completing the inductive step.

3. (i) As noted the second statement that $n \cdot (m \cdot r) = (nm) \cdot r$ holds in any abelian group. To see the first statement, it clearly holds for $n = 0$ (all terms are 0) and $n = 1$ (all terms are rs). To see it for all $n > 0$, assume inductively that it has been proved for n. Then

$$((n+1)\cdot r)s = (n\cdot r+r)\cdot s = (n\cdot r)s+rs = r(n\cdot s)+rs = r(n\cdot s+s) = r((n+1)\cdot s).$$

The argument that $((n+1)\cdot r)s = (n+1)\cdot(rs)$ is similar. This establishes the result for all $n \geq 0$ which was all that the problem asked for. To establish the result for $n < 0$, write $n = -m$ with $m > 0$, and use the law of exponents $(-m) \cdot r = -(m \cdot r)$ along with (for example):

$$\begin{aligned}(n \cdot r)s &= ((-m) \cdot r)s = (-(m \cdot r))s = -(m \cdot r)s \\ &= -r(m \cdot s) = r(-(m \cdot s)) = r((-m) \cdot s) = r(n \cdot s).\end{aligned}$$

(ii): Clearly (laws of exponents again)

$$f(n + m) = (n + m) \cdot 1 = (n \cdot 1) + (m \cdot 1) = f(n) + f(m).$$

To see that f is multiplicative,

$$f(nm) = (n \cdot 1)(m \cdot 1) = 1(n \cdot (m \cdot 1)) = (n \cdot (m \cdot 1)) = (nm) \cdot 1,$$

where the last step also uses the laws of exponents. Finally, $f(1) = 1 \cdot 1 = 1$. The statement about the image of f is obvious by definition. Finally, if g is any homomorphism from $\mathbb{Z}$ to R, then $g(1) = 1$ by our conventions, hence $g(n) = n \cdot 1$ for all $n \in \mathbb{Z}$, hence $g = f$.

4. (a) $(r + s)(r - s) = r^2 + sr - rs - s^2 = r^2 - s^2$. In fact, from the above, we see that R is commutative $\iff$ $(r + s)(r - s) = r^2 - s^2$ for all $r, s \in R$. (b) $(r + s)^2 = r^2 + sr + rs + s^2 = r^2 + 2 \cdot rs + s^2$; the first equality is all you can say in a general (noncommutative) ring. (c) By induction on n, starting for example with the case $n = 1$. The inductive step is

$$\begin{aligned}(r + s)^{n+1} &= (r + s)(r + s)^n = (r + s) \sum_{i=0}^{n} \binom{n}{i} \cdot r^i s^{n-i} \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot r^{i+1} s^{n-i} + \sum_{i=0}^{n} \binom{n}{i} \cdot r^i s^{n+1-i},\end{aligned}$$

and the formula follows with a little manipulation of the indices from the usual identity between binomial coefficients $\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$.

5. (a) $\alpha\bar{\alpha} = (x_0 + x_1 i + x_2 j + x_3 k)(x_0 - x_1 i - x_2 j - x_3 k)) = x_0^2 + x_0(x_1 i + x_2 j + x_3 k) + x_0(-x_1 i - x_2 j - x_3 k) + (x_1 i)(-x_1 i) + x_1 i(-x_2 j) + x_2 j(-x_1 i) + x_1 i(-x_3 k) + x_3 k(-x_1 i) + x_2 j(-x_2 j) + x_2 j(-x_3 k) + x_3 k(-x_2 j) + x_3 k(-x_3 k)$. Using the fact that $ij + ji = ik + ki = jk + kj = 0$, it is easy to see that all terms cancel except $x_0^2 + (x_1 i)(-x_1 i) + x_2 j(-x_2 j) + x_3 k(-x_3 k) = x_0^2 + x_1^2 + x_2^2 + x_3^2$. If $\alpha \neq 0$, $|\alpha| \neq 0$, and $\alpha \cdot (\bar{\alpha}/|\alpha|^2) = 1$. (b) Using (a) (or directly) $\alpha^2 = (\alpha)(-\bar{\alpha}) = -|\alpha|^2 = -x_1^2 - x_2^2 - x_3^2$. Since there are an infinite number of $(x_1, x_2, x_3) \in \mathbb{R}^3$ such that $x_1^2 + x_2^2 + x_3^2 =$ (this is just the unit sphere in $\mathbb{R}^3$), there are an infinite number of $\alpha \in \mathbb{H}$ with $\alpha^2 = -1$.

6. $Z(R)$ is an additive subgroup: given $r_1, r_2 \in Z(R)$, $(r_1 + r_2)s = r_1 s + r_2 s = s r_1 + s r_2 = s(r_1 + r_2)$ for all $s \in R$. Hence $r_1 + r_2 \in Z(R)$ by definition. Clearly $0s = 0 = s0$ for all $s \in R$, so that $0 \in Z(R)$, and, for $r \in Z(R)$ and for all $s \in R$, $(-r)s = -(rs) = -(sr) = s(-r)$. Hence $Z(R)$ is an additive subgroup. $Z(R)$ is closed under multiplication: given $r_1, r_2 \in Z(R)$ and $s \in R$, $(r_1 r_2)s = r_1(r_2 s) = r_1(s r_2) = (r_1 s) r_2 = (s r_1) r_2 = s(r_1 r_2)$ via multiple applications of associativity. Clearly, if there exists a unity $1 \in R$, then by definition $1 \cdot s = s = s \cdot 1$ for all $s \in R$, so that $1 \in Z(R)$. If $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in Z(\mathbb{H})$, then using $\alpha i = i\alpha$, $\alpha j = j\alpha$, we see that $x_1 = x_2 = x_3 = 0$, hence $\alpha = x_0 \in \mathbb{R}$. Conversely, $t \in \mathbb{R}$ commutes with every element of $\mathbb{H}$, hence $Z(\mathbb{H}) = \mathbb{R}$.

Second problem set

1. (i) Let $a + bi \in \mathbb{Z}[i]$, $a + bi \neq 0$, and suppose that $(a + bi)^{-1}$ is also in $\mathbb{Z}[i]$. Then

$$\frac{1}{a+bi} = \frac{1}{a+bi}\left(\frac{a-bi}{a-bi}\right) = \frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}.$$

Thus $a/(a^2 + b^2) \in \mathbb{Z}$. But $|a| \leq a^2$, and hence $|a| \leq a^2 + b^2$, with equality $\iff b = 0$ and $a = 0, \pm 1$. Thus $0 \leq |a|/(a^2 + b^2) \leq 1$, and since $|a|/(a^2 + b^2) \in \mathbb{Z}$, either $a = 0$ or $a = \pm 1$ and $b = 0$. Likewise either $b = 0$ or $b = \pm 1$ and $a = 0$. Since not both a, b are 0, one is 0 and the other is ± 1, leading to the four possibilities ± 1, $\pm i$. Since all four of these are units, $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$.

(ii) By direct calculation,

$$\frac{1}{1+\sqrt{2}} = \frac{1}{1+\sqrt{2}}\left(\frac{1-\sqrt{2}}{1-\sqrt{2}}\right) = \frac{1}{1-2} - \frac{\sqrt{2}}{1-2} = -1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Hence $1+\sqrt{2} \in (\mathbb{Z}[\sqrt{2}])^*$. Since clearly $1+\sqrt{2} > 1$, $(1+\sqrt{2})^n > 1$ for all $n \in \mathbb{N}$, hence $1+\sqrt{2}$ is of infinite order in the multiplicative group $(\mathbb{Z}[\sqrt{2}])^*$. (In fact, one can show that $(\mathbb{Z}[\sqrt{2}])^* \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$.)

2. (a) By inspection, the binomial coefficient is an integer r of the form pa/b, where $a, b \in \mathbb{N}$ and p does not divide b. Hence $pa = br$, so that $p|br$. Since p does not divide b, $p|r$. (b) Follows immediately from the binomial theorem and the fact that, in R, $(pn) \cdot r = n \cdot (p \cdot r) = 0$ for all $r \in R$. (c) By Part (b), $F(r+s) = F(r) + F(s)$, and clearly $F(rs) = (rs)^p = r^p s^p = F(r)F(s)$. Finally $F(1) = 1^p = 1$, so F is a homomorphism. If R is an integral domain (or more generally contains no nilpotent elements other than 0), then $F(r) = 0 \iff r^p = 0 \iff r = 0$. Hence $\operatorname{Ker} F = \{0\}$ so that F is injective. (d) By Fermat's little theorem, for all $a \in \mathbb{F}_p$, $a^p = a$, hence $F = \mathrm{Id}$. (This also follows from the fact that F is a homomorphism such that $F(1) = 1$.) (e) F is injective because R is an integral domain (or directly from the following). If $f(x) = \sum_{i=0}^n a_i x^i$, then

$$F(f) = (\sum_{i=0}^n a_i x^i)^p = \sum_{i=0}^n a_i^p (x^i)^p = \sum_{i=0}^n a_i x^{ip} = f(x^p).$$

Thus the image of F is the subring $\mathbb{F}_p[x^p]$ of $\mathbb{F}_p[x]$ consisting of all polynomials in x^p.

3. (a) If $r^N = 0$, then $(sr)^N = s^N r^N = 0$. (b) Suppose that $r^N = 0$, $s^M = 0$. If $D \in \mathbb{N}$ and $D \geq N + M - 1$, then $(r+s)^D = \displaystyle\sum_{k=0}^{D} \binom{D}{k} \cdot r^k s^{D-k}$. If $k \geq N$, then $r^k = 0$. If $k < N$, then $k \leq N-1$, and hence $D - k \geq M$, so that $s^{D-k} = 0$. So all of the terms of the sum are 0, and hence $(r+s)^D = 0$. (c) Suppose that $r \in R$ and $r^N = 0$ for some $N \geq 1$. By induction, in any ring with unity, $(1-a)(1+a+\cdots+a^n) = 1 - a^{n+1}$. Applying this to $a = -r$ and $n = N-1$ gives

$$(1+r)\left(\sum_{k=0}^{N-1}(-1)^k r^k\right) = 1 - (-1)^N r^N = 1.$$

Thus $1+r$ is a unit. The case of $u+r$, u a unit, follows by writing $u + r = u(1+u^{-1}r)$. Then $u^{-1}r$ is nilpotent by (a), $1+u^{-1}r$ is a unit by the first part of (c), and hence $u + r = u(1+u^{-1}r)$ is a unit since it is a product of units. (d) By (a), rx is nilpotent and by (c) $1+rx$ is a unit. (In fact, a much more difficult argument shows that, if R is a commutative ring with unity, then a polynomial $\sum_{k=0}^N a_k x^k \in R[x]$ is a unit in $R[x] \iff a_0 \in R^*$ and a_i is nilpotent for $i > 0$.)

4. Divisors of zero: the nonzero elements $a \in \mathbb{Z}/n\mathbb{Z}$ such that $d = \gcd(a, n) > 1$, since then $a \cdot (n/d) = 0$ in $\mathbb{Z}/n\mathbb{Z}$ but $n/d \neq 0$. Nilpotent elements: if $n = p_1^{a_1} \cdots p_r^{a_r}$ is the factorization on n into a product of distinct prime powers (i.e. $p_i \neq p_j$ for $i \neq j$ and $a_i \geq 1$), then a is nilpotent $\iff$ a is divisible by $p_1 \cdots p_r$, i.e. any prime which divides n must divide a. To see this, if $p_1 \cdots p_r | a$ and $N = \max\{a_1, \dots, a_r\}$, then clearly $n | (p_1 \cdots p_r)^N | a^N$ so a is nilpotent. Conversely, if a is nilpotent, say $a^N = 0$ in $\mathbb{Z}/n\mathbb{Z}$, then for all i $p_i | n | a^N$. and hence $p_i | a$.

5. Note that $a \pm bi$ is not zero as long as at least one of a, b is nonzero: this is clear if $a = 0$, $b \neq 0$ or $b = 0$, $a \neq 0$, and if both are nonzero it is just the statement that i is not a rational number $\pm a/b$. Then

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{bi}{a^2 + b^2} \right) = \frac{a^2 + b^2}{a^2 + b^2} + \frac{abi - abi}{a^2 + b^2} = 1.$$

The case of $\mathbb{Q}(\sqrt{2})$ is similar, noting that, since $\sqrt{2} \notin \mathbb{Q}$, $a \pm b\sqrt{2}$ is nonzero as long as at least one of a, b is nonzero, in which case $a^2 - 2b^2$ is also nonzero. Then

$$(a + b\sqrt{2}) \cdot \left(\frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2} \right) = \frac{a^2 - 2b^2}{a^2 - 2b^2} + \frac{ab\sqrt{2} - ab\sqrt{2}}{a^2 - 2b^2} = 1.$$

6. To do this (lengthy) computation, it helps to organize it, say in terms of the coefficients of 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$. For example, the terms that give a rational number can be grouped as

$$\begin{aligned} a(a^2 - 2bc) + b\sqrt[3]{2}(b^2 - ac)(\sqrt[3]{2})^2 + c(\sqrt[3]{2})^2(-ab + 2c^2)(\sqrt[3]{2}) \\ = a^3 - 2abc + 2(b^3 - abc) + 2(-abc + 2c^3) \\ = a^3 + 2b^3 + 4c^3 - 6abc. \end{aligned}$$

Similarly, the coefficients of $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2$ are 0. (Note: to see that $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$ as long as one of a, b, c is nonzero, it is enough to check that $(a^2 - 2bc) + (-ab + 2c^2)(\sqrt[3]{2}) + (b^2 - ac)(\sqrt[3]{2})^2 \neq 0$ in this case. As we shall see shortly in class, $(a^2 - 2bc) + (-ab + 2c^2)(\sqrt[3]{2}) + (b^2 - ac)(\sqrt[3]{2})^2 = 0$ $\iff$ all of the coefficients are 0 $\iff$ a, b, c satisfy the system of equations $a^2 = 2bc$, $2c^2 = ab$, $b^2 = ac$. So we must show that the only solution of these equations is $a = b = c = 0$. This is a straightforward argument, using the fact that $\sqrt[3]{2}$ is irrational.)