

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 of 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: $a_1/b_1 + a_2/b_2 = (a_1 b_2 + a_2 b_1)/(b_1 b_2)$, and, if 2 does not divide b_1 or b_2 , then 2 does not divide the product $b_1 b_2$. 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 $a_1/b_1 \cdot a_2/b_2 = (a_1 a_2)/(b_1 b_2)$, and as before if 2 does not divide b_1 or b_2 , then 2 does not divide $b_1 b_2$. 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. 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):

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

For the last part, 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.

3. (i) We must have $f(1) = (1, 1)$, hence $f(n) = n \cdot (1, 1) = (n, n)$ and by Problem 2 this is indeed a homomorphism, hence the unique such. (ii) We must have $f(1) = 1$, hence $f(n) = n \cdot 1$ and by Problem 2 this is indeed a homomorphism, hence the unique such. (iii) Since $f(n, m) = nf(1, 0) + mf(0, 1)$, f is specified by its values on $(1, 0)$ and $(0, 1)$. We must have $f(1, 1) = 1$, but this does not specify f . Also, $f(1, 0) = f((1, 0)^2) = (f(1, 0))^2$, so that $f(1, 0)$ is an integer x such that $x^2 = x$, hence $x = 0$ or 1 . Similarly $f(0, 1)$ is 0 or 1 . Finally, since $f(1, 0) + f(0, 1) = f(1, 1) = 1$, one of $f(1, 0)$ is 0 and the other is 1 . In the first case $f(n, m) = n$ and in the second case $f(n, m) = m$; both of these are easily checked to be homomorphisms.

If we look at functions $f: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ which are additive homomorphisms and which satisfy $f(nm) = f(n)f(m)$, but not necessarily $f(1) = 1$, we see that $f(1) = f(1^2) = (f(1))^2$. Thus if $f(1) = (a, b)$, then $a^2 = a$ and $b^2 = b$, so a is 0 or 1 and b is 0 or 1 . This gives 4 possibilities for f : $f(n) = 0$ always, $f(n) = (n, 0)$, $f(n) = (0, n)$, and $f(n) = (n, n)$. All 4 possibilities are easily checked to be homomorphisms.

5. $Z(R)$ is an additive subgroup: given $r_1, r_2 \in Z(R)$, $(r_1 + r_2)s = r_1s + r_2s = sr_1 + sr_2 = s(r_1 + r_2)$ 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 $s \in R$, $(r_1r_2)s = r_1(r_2s) = r_1(sr_2) = (r_1s)r_2 = (sr_1)r_2 = s(r_1r_2)$ 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 $1 \in Z(R)$.

6. (a) $(r+s)(r-s) = r^2 + sr - rs - s^2 = r^2 - s^2$. (b) $(r+s)^2 = r^2 + sr + rs + s^2 = r^2 + 2 \cdot rs + s^2$. (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 $\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$.

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 $\pm 1, \pm i$. 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 $\text{Ker } F = \{0\}$ so that F is injective. (d) By Fermat's little theorem, for all $a \in \mathbb{F}_p$, $a^p = a$, hence $F = \text{Id}$. (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

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

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. If $f(x), g(x) \in R[x]$ and $f(x)g(x) = 1$, then neither $f(x)$ nor $g(x)$ is 0, hence both have a well-defined degree and $\deg f(x) + \deg g(x) = \deg 1 = 0$. Hence $\deg f(x) = \deg g(x) = 0$, i.e. $f(x) = r, g(x) = s$ for some $r, s \in R$ (they are constant polynomials). Since $rs = 1$, $r \in R^*$. Conversely, if $r \in R^*$, then r is clearly a unit in $R[x]$.

4. (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 $(r + s)^D = \sum_{k=0}^D \binom{D}{k} \cdot r^k s^{D-k}$. 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 $i > 0$.) (e) Follows by direct computation (the invertibility of $A + B$ follows since $\det(A + B) = -1$ or by writing out the inverse explicitly).

5. 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 $p_i | a$.