Math 430 – Problem Set 5 Solutions

Due April 1, 2016

13.2. Find all of the abelian groups of order 200 up to isomorphism.

Solution. Every abelian group is a direct product of cyclic groups. Using the fact that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$, the list of groups of order 200 is determined by the factorization of 200 into primes:

- $\mathbb{Z}_8 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

13.5. Show that the infinite direct product $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ is not finitely generated.

Solution. Note that every element of G has order 2 and that G is abelian. The group generated by any finite set of k elements thus has at order at most 2^k, while G has infinite order. Thus G cannot be finitely generated.

16.1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) $7\mathbb{Z}$

Solution. The is a subring of $\mathbb{Z}$ and thus a ring:

- $(7n) + (7m) = 7(m + n)$ so it is closed under addition;
- $(7n)(7m) = 7(7mn)$ so it is closed under multiplication;
- $-(7n) = (-7)(n)$, so it is closed under negation.

It is not a field since it does not have an identity.

(b) $\mathbb{Z}_{18}$

Solution. This is a ring: the operations of arithmetic modulo 18 are well defined. It is not a field, since $2 \cdot 9 = 0$ gives a pair of zero divisors.

(c) $\mathbb{Q}(\sqrt{2})$

Solution. This is a subfield of $\mathbb{R}$ and thus a field (in addition to being a ring:

- $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ so it is closed under addition;
- $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ so it is closed under multiplication;
- $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$ so it is closed under negation;
- $(a + b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ and $a^2 - 2b^2 \neq 0$ for $a, b \in \mathbb{Q}$ (unless both are zero)

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

Solution. This is not a ring since $\sqrt[3]{3} \cdot \sqrt[3]{3}$ is not in R.

(h) $\mathbb{Q}(\sqrt[3]{3})$

Solution. This is a subfield of $\mathbb{R}$ and thus a field:

- $(a + b\sqrt[3]{3} + c\sqrt[3]{9}) + (d + e\sqrt[3]{3} + f\sqrt[3]{9}) = (a + d) + (b + e)\sqrt[3]{3} + (c + f)\sqrt[3]{9}$ so it is closed under addition;
- $(a+b\sqrt[3]{3}+c\sqrt[3]{9})(d+e\sqrt[3]{3}+f\sqrt[3]{9}) = (ad+3bf+3ce)+(ae+bd+3cf)\sqrt[3]{3}+(af+be+cd)\sqrt[3]{9}$ so it is closed under multiplication;
- $-(a + b\sqrt[3]{3} + c\sqrt[3]{9}) = (-a) + (-b)\sqrt[3]{3} + (-c)\sqrt[3]{9}$ so it is closed under negation.
- Closure under inverses takes a bit more work, since there is no single conjugate. We give two arguments.
  i. In our first approach, we show directly that each element has an inverse. Given $(a+b\sqrt[3]{3}+c\sqrt[3]{9})$ we prove that there is some $(d+e\sqrt[3]{3}+f\sqrt[3]{9})$ with $(a+b\sqrt[3]{3}+c\sqrt[3]{9})(d+e\sqrt[3]{3}+f\sqrt[3]{9}) = 1$ using the formula for multiplication above. This requires solving

$$\begin{aligned} ad + 3ce + 3bf &= 1 \\ bd + ae + 3cf &= 0 \\ cd + be + af &= 0. \end{aligned}$$

  This system will have a solution as long as the determinant

$$\det \begin{pmatrix} a & 3c & 3b \\ b & a & 3c \\ c & b & a \end{pmatrix} = a^3 + 3b^3 + 9c^3 - 9abc$$

  is nonzero. Multiplying all of a, b and c by a common rational value we may assume that they are all integers and share no common factor. If $a^3 + 3b^3 + 9c^3 - 9abc = 0$ then a^3 is a multiple of 3, and thus a is by unique factorization (say $a = 3a'$). Then

$$9a'^3 + b^3 + 3c^3 - 9a'bc = 0.$$

  Repeating this for b and c, we see that all are divisible by 3, contradicting the fact that we chose them to have no common factor.

  ii. The other approach uses the extended Euclidean algorithm for polynomials. Since $\sqrt[3]{3}$ is irrational, $x^3 - 3$ is irreducible and thus $\gcd(x^3 - 3, a + bx + cx^2) = 1$. Therefore, there exist $f(x), g(x) \in \mathbb{Q}[x]$ with

$$f(x)(x^3 - 3) + g(x)(a + bx + cx^2) = 1.$$

  Evaluating this equation at $x = \sqrt[3]{3}$ shows that $g(\sqrt[3]{3})$ is the inverse of $a + b\sqrt[3]{3} + c\sqrt[3]{9}$.

16.2. Let R be the ring of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a subring S of R with an identity.

Solution. Suppose that $\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right)$ is an identity for R. Then

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \end{aligned}$$

so $a = 1$ and $b = 1$. But $\left(\begin{smallmatrix}1 & 1\\ 0 & 0\end{smallmatrix}\right)$ is not an identity, since

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}.$$

Thus R has no identity.

Let S be the subring of matrices of the form $\left(\begin{smallmatrix}a & 0\\ 0 & 0\end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$ is an identity for S, since

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix},$$
$$\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}.$$

16.6. Find all homomorphisms $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

Solution. Since ϕ is a ring homomorphism, it must also be a group homomorphism (of additive groups). Thuso $6\phi(1) = \phi(0) = 0$, and therefore $\phi(1) = 0, 5$ or 10 (and ϕ is determined by $\phi(1)$). If $\phi(1) = 5$, then

$$\begin{aligned}\phi(1) &= \phi(1 \cdot 1)\\ &= \phi(1) \cdot \phi(1)\\ &= 5 \cdot 5\\ &= 10,\end{aligned}$$

which is a contradiction. So the only two possibilities are

$$\begin{aligned}\phi_1(n) &= 0 \text{ for all } n \in \mathbb{Z}_6.\\ \phi_2(n) &= 10n \text{ for all } n \in \mathbb{Z}_6.\end{aligned}$$

We show that these are both well defined ring homomorphisms.

In both cases, adding a multiple of 6 to n changes the result by a multiple of 15 (0 in the first case and 60 in the second), so they are well defined. They are additive group homomorphisms by the distributive law in $\mathbb{Z}_{15}$. They are multiplicative since

$$\begin{aligned}0 \cdot 0 &= 0\\ (10n) \cdot (10m) &= 100nm = 10nm.\end{aligned}$$

16.10. Define a map $\phi : \mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ by

$$\phi(a + bi) = \begin{pmatrix}a & b\\ -b & a\end{pmatrix}.$$

Show that ϕ is an isomorphism of $\mathbb{C}$ with its image in $\mathbb{M}_2(\mathbb{R})$.

Solution. We first show that ϕ is a homomorphism.

$$\begin{aligned}
\phi((a+bi)+(c+di)) &= \phi((a+c)+(b+d)i) \\
&= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \\
\phi(a+bi)+\phi(c+di) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
&= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \\
\phi((a+bi)(c+di)) &= \phi((ac-bd)+(ad+bc)i) \\
&= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} \\
\phi(a+bi)\phi(c+di) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
&= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}
\end{aligned}$$

Finally, we show that ϕ is injective and thus an isomorphism onto its image. If $\phi(a+bi) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ then $a = 0$ and $b = 0$.

16.17. Let a be any element in a ring R with identity. Show that $(-1)a = -a$.

Solution. We have

$$\begin{aligned}
(-1)a + a &= (-1)a + (1)a \\
&= (-1+1)a \\
&= (0)a \\
&= 0.
\end{aligned}$$

The result now follows from the uniqueness of additive inverses.

16.22. Prove the Correspondence Theorem: Let I be an ideal of a ring R. Then $S \to S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R correspond to the ideals of R/I.

Solution.

- We first show that the function $S \mapsto S/I$ sends subrings of R to subrings of R/I. If $s, t \in S$ then $(s+I)+(t+I) = (s+t)+I \in S/I$ since S is closed under addition, $(s+I)(t+I) = (st)+I \in S/I$ since S is closed under multiplication and $-(s+I) = (-s)+I \in S/I$ since S is closed under negation. Thus S/I is a subring.
- We now show that this function is surjective. Let $T \subseteq R/I$ be a subring and set $S = \{x \in R : x+I \in T\}$. Then S is a subring of R: if $s, t \in S$ then $s+t \in S$ since $(s+t)+I = (s+I)+(t+I)$ and T is closed under addition, $st \in S$ since $(st)+I = (s+I)(t+I)$ and T is closed under multiplication, and $-s \in S$ since $(-s)+I = -(s+I)$ and T is closed under negation. Moreover, S contains I since $i+I = 0+I \in T$ for every $i \in I$. Finally, $S/I = T$ by construction.
- Next, we show that this function is injective. Suppose S_1 and S_2 are two subrings of R that contain I and that $S_1/I = S_2/I$ inside R/I. We show that $S_1 \subseteq S_2$ (the opposite inclusion is analogous). Suppose $x \in S_1$. Since $S_1/I = S_2/I$, there is some $y \in S_2$ with $x+I = y+I$. Thus there is an $i \in I$ with $x = y+i$. Since $I \subseteq S_2$, both y and i are in S_2 and thus x is as well.

- Next, suppose that S is actually an ideal of R. To show that S/I is an ideal of R/I, we take an arbitrary $s + I \in S/I$ and $x + I \in R/I$. Then $xs + I \in S/I$ and $sx + I \in S/I$ since S is an ideal of R.
- Finally, suppose that $T \subseteq R/I$ is an ideal. Let $S = \{x \in R : x + I \in T\}$ as before. We show that S is an ideal of R, proving that the correspondence restricts to a correspondence on ideals. If $s \in S$ and $x \in R$ then $xs + I = (x + I)(s + I) \in S/I$ since S/I is an ideal; similarly for sx. Thus S is an ideal.

16.26. Let R be an integral domain. Show that if the only ideals in R are $\{0\}$ and R itself, R must be a field.

Solution. In order to show that R is a field it suffices to prove that every nonzero $a \in R$ has an inverse. Let $a \in R$ be nonzero, and consider the ideal $\langle a \rangle$ generated by a. Since $a \neq 0$, this ideal is nonzero and thus is all of R by assumption. Therefore it contains 1; by the definition of a principal ideal there is some $b \in R$ with $ab = 1$, providing the inverse of a.

16.31. Let R be a ring such that $1 = 0$. Prove that $R = \{0\}$.

Solution. If $a \in R$ then $a = (1)a = (0)a = 0$, so $R = \{0\}$.

16.34. Let p be a prime. Prove that

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z} \text{ and } \gcd(b, p) = 1\}$$

is a ring.

Solution. We show that this is a subring of $\mathbb{Q}$ and thus a ring. If $a/b, c/d \in \mathbb{Z}_{(p)}$ to show that $a/b + c/d = (ad + bc)/(bd)$ and $(a/b)(c/d) = ac)/(bd) \in \mathbb{Z}_{(p)}$ it suffices to show that $\gcd(bd, p) = 1$. This follows from the fact that p is prime: if it does not divide b or d then it cannot divide bd. Negation is even easier: $-(a/b) = (-a)/b \in \mathbb{Z}_{(p)}$ since it has the same denominator.

16.38. An element x in a ring is called an idempotent if $x^2 = x$. Prove that the only idempotents in an integral domain are 0 and 1. Find a ring with an idempotent x not equal to 0 or 1.

Solution. If $x^2 = x$ then $(x - 1)x = x^2 - x = 0$. An integral domain has no zero divisors, so the only possibilities for x are 0 and 1.

$3 \in \mathbb{Z}_6$ is an example of an idempotent that is neither 0 nor 1.