ALGEBRA FINAL SOLUTIONS

No books or notes.
Maximal Score: 215.

He who learns but does not think is lost. He who thinks but
does not learn is in great danger. – Confucius

PART I: DO ANY THREE OF THESE FOUR PROBLEMS

1. (30) Let $G$ be an group under multiplication. Set
   $H = \{x \in G : x^n = 1 \text{ for some } n \geq 1\}$

   (a) (15) Assume $G$ is Abelian. Prove that $H$ is a subgroup of $G$. Point
   out in your argument where you needed that $G$ was Abelian.
   Solution: As usual there are three parts:
   Identity: As $1^1 = 1$, $1 \in H$
   Product: Let $x, y \in H$. Then there exist $n, m$ with $x^n = 1$ and $y^m = 1$. (Warning: You cannot assume $n, m$ are the same!).
   Then
   \[(xy)^mn = x^mn^m = (x^n)^m(y^m)^n = 1^m1^n = 1\]
   so $xy \in H$. (Abelian was used to say $(xy)^mn = x^mn^m$.)
   Inverse: Let $x \in H$. Then $x^n = 1$ for some $n$. Then $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$ so $x^{-1} \in H$.

   (b) (10) Now do not assume $G$ is Abelian but assume that $H$ is a
   subgroup of $G$. Prove that $H$ is a normal subgroup of $G$.
   Solution: Let $h \in H$ and $g \in G$. So $h^n = 1$ for some $n$. Then
   \[(g^{-1}hg)^n = g^{-1}h^ng = g^{-1}1g = g^{-1}g = 1\]
   (as in $(g^{-1}hg)^n$ the inner $gg^{-1}$ terms all cancel) and so $g^{-1}hg \in H$

   (c) (5) Now do not assume $G$ is Abelian but assume that $G$ is finite.
   In this case $H$ has a “trivial” value. What is it, and why?
   Solution: $H = G$ as for all $x \in G$, $x^{o(G)} = 1$.

2. (30) Let $G = Z[\sqrt{2}]$ and let $H = (2 + \sqrt{2})$. 

1
(a) (10) Mark the points \((a, b)\) with \(-4 \leq a, b \leq +4\) so that \(a + b\sqrt{2} \in H\).

**Solution:** We have \(2 = (2 + \sqrt{2})(2 - \sqrt{2})\) and \(\sqrt{2} = (2 + \sqrt{2})(-1 + \sqrt{2})\) so you get every other point on the X-axis, and when you have a point you get the entire Y-line. The answer is

```
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
xoxoxoxoxox
```

where X is the origin and the points of \(H\) are marked by \(x\).

(b) (10) Find a natural set of coset representatives for \(G/H\).

**Solution:** \(0, 1\) are coset representatives.

(c) (10) Is \(G/H\) a field? What well known structure is \(G/H\) isomorphic to?

**Solution:** \(G/H \cong \mathbb{Z}_2\) and is a field.

3. (30) Let \(R\) be an integral domain. For any \(\alpha, \beta \in R\) define

\[
(\alpha, \beta) = \{m\alpha + n\beta : m, n \in R\}
\]

(a) (10) Prove \((\alpha, \beta)\) is an ideal.

**Solution:** Set \(I = (\alpha, \beta)\). There are four parts:

- **Identity:** \(0 = 0\alpha + 0\beta \in I\).
- **Additive Inverse:** If \(x = m\alpha + n\beta \in I\) then \(-x = (-m)\alpha + (-n)\beta \in I\).
- **Addition Closure:** If \(x = m\alpha + n\beta \in I\) and \(y = m'\alpha + n'\beta \in I\) then \(x + y = (m + m')\alpha + (n + n')\beta \in I\).
- **The Big One:** Let \(x \in I\) and \(r \in R\). Then \(x = m\alpha + n\beta \in I\) so \(rx = (rm)\alpha + (rn)\beta \in I\).

(b) (20) Let \(a, b, c, d \in R\) with \(ad - bc\) a unit of \(R\). Prove \((\alpha, \beta) = (a\alpha + b\beta, c\alpha + d\beta)\).

**Solution:** Let \(x \in (a\alpha + b\beta, c\alpha + d\beta)\). So

\[
x = m(a\alpha + b\beta) + n(c\alpha + d\beta) = (ma + cn)\alpha + (mb + nd)\beta \in (\alpha, \beta)
\]

Thus \((a\alpha + b\beta, c\alpha + d\beta) \subseteq (\alpha, \beta)\). Now the hard part. Let \(y \in (\alpha, \beta)\) so that \(y = r\alpha + s\beta\). We want to show that \(y \in (a\alpha + b\beta, c\alpha + d\beta)\). For any \(m, n\) we have \((ma + cn)\alpha + (mb + nd)\beta \in (ma + cn)\alpha + (mb + nd)\beta\). So it suffices to show that there exist \(m, n\) with

\[
am + cn = r
bm + dn = s
\]
We employ linear algebra. Multiply the first equation by \(d\) and the second by \(-c\) and add getting

\[(ad - bc)m = dr - cs\]

Similarly, multiply the first equation by \(b\) and the second by \(-a\) and add getting

\[(bc - ad)n = br - as\]

Our solution is then

\[m = \frac{dr - cs}{ad - bc} \quad \text{and} \quad n = \frac{as - br}{ad - bc}\]

which exist in \(R\) as \(ad - bc\) is assummed to be a unit.

4. (30) Let \(d\) be a positive integer which is not a square and set \(R = \mathbb{Z}[\sqrt{d}]\). Let \(U\) be the set of units of \(R\).

(a) (5) Prove that if \(x^2 - dy^2 = +1\) or \(-1\) then \(x + y\sqrt{d} \in U\).

Solution: If \((x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 = \pm1\) so the inverse of \(x + y\sqrt{d}\) is either \(x - y\sqrt{d}\) or its negative.

(b) (10) Prove that if \(x + y\sqrt{d} \in U\) then \(x^2 - dy^2 = +1\) or \(-1\).

Solution: Set \(d(x + y\sqrt{d}) = |x^2 - dy^2|\). Say \(\alpha = x + y\sqrt{d} \in U\) with \(\alpha\beta = 1\). Then \(1 = d(\alpha\beta) = d(\alpha)d(\beta)\) so, as \(d(\cdot)\) is a positive integer both factors must by one and so \(d(\alpha) = 1\) so \(|x^2 - dy^2| = 1\) so \(x^2 - dy^2 = +1\) or \(-1\).

(c) (15) Prove that \(U \cong \mathbb{Z} \times \mathbb{Z}_2\) (both \(\mathbb{Z}\) and \(\mathbb{Z}_2\) under addition).

You may, and should, use results proven in Prof. Venkatesh’s guest lecture.

Solution: Prof. Venkatesh showed there was a fundamental unit \(\epsilon\) so that all elements of \(U\) can be uniquely written as \(\pm\epsilon^n\) for \(n \in \mathbb{Z}\). For the isomorphism we map \(\pm\epsilon^n\) into \((n, \delta)\) where \(\delta = 0\) when the sign is positive and \(\delta = 1\) when the sign is negative.

**PART II: DO ANY THREE OF THESE FOUR PROBLEMS**

5. (15) Find the inverse of \(1 + x\) in \(\mathbb{Z}_3[x]/(x^3 + 2x + 2)\).

Solution: We use the method of undetermined coefficients.

\[1 = (1 + x)(a + bx + cx^2) = a + (a + b)x + (b + c)x^2 + cx^3\]

But \(x^3 + 2x + 2 = 0\) implies \(x^3 = x + 1\) so

\[1 = a + (a + b)x + (b + c)x^2 + c(x + 1) = (a + c) + (a + b + c)x + (b + c)x^2\]

which gives the three equation

\[1 = a + c\]
\[0 = a + b + c\]
\[0 = b + c\]

The second minus the first gives \(b = -1 = 2\), then the third gives \(c = 1\) and the first gives \(a = 0\) so the answer is \(0 + 2x + x^2\).
6. (15) In $\mathbb{Z}[i]$ apply the Euclidean Algorithm to find $\gcd(5 + 3i, 1 + 5i)$.

**Solution:**

\[
\begin{align*}
5 + 3i & = \frac{5 + 3i}{1 + 5i} \left(1 - i\right) + \frac{20 - 22i}{26} \\
1 + 5i & = \frac{1 + 5i}{-1 - i} \left(-1 - i\right) + \frac{20 - 22i}{26}
\end{align*}
\]

so we take $q = 1 - i$ and $r = (5 + 3i) - (1 + 5i)q$ so that

\[5 + 3i = (1 - i)(1 + 5i) + (1 - i)\]

Now we divide $1 + 5i$ by $-1 - i$.

\[
\begin{align*}
1 + 5i & = \frac{1 + 5i}{-1 - i} \left(-1 - i\right) + \frac{-6 - 4i}{2} = -3 - 2i
\end{align*}
\]

So we have

\[1 + 5i = (-3 - 2i)(1 - i)\]

and we are done. The gcd is the last nonzero remainder which is $1 - i$.

7. (15) Let $G$ be an Abelian group (under multiplication) with $n$ elements. Suppose $G$ is not isomorphic to $(\mathbb{Z}_n, +)$. Show that there is an $r < n$ so that $x^r = 1$ for all $x \in G$. (You may, and should, use results shown in class about Finite Abelian Groups.)

**Solution:** We showed in class that $G \cong \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s}$ where each $a_i$ divides the next. As $G$ is not isomorphic to $\mathbb{Z}_n$ we must have $s > 1$. On the right hand side (under addition) we have $a_s u = 0$ for all $u$ so on the left hand side (under multiplication) we have $x^{a_s} = 1$ for all $x \in G$. (Remark: This result is used to prove that the multiplicative group of a finite field is cyclic. The idea is that otherwise, letting $n$ be the number of elements of that multiplicative field, $x^r = 1$ would have $n$ solutions in the field. Stick around for Algebra II and you’ll see that can’t be.)

8. (15) Let $G$ be a group and $g \in G$. Define $\phi : G \rightarrow G$ by $\phi(x) = g^{-1}xg$.

(a) (5) Prove $\phi$ is a homomorphism.

**Solution:** $\phi(x)\phi(y) = g^{-1}xgg^{-1}yg = g^{-1}(xy)g = \phi(xy)$.

(b) (5) Prove $\phi$ is injective.

**Solution:** Suppose $e = \phi(x) = g^{-1}xg$. Left multiplying by $g$ and right multiplying by $g^{-1}$ gives $e = gg^{-1} = gg^{-1}xgg^{-1} = x$.

(c) (5) Prove $\phi$ is surjective.

**Solution:** Let $y \in G$. We need find $x$ with $y = \phi(x) = g^{-1}xg$. Take $x = ggy^{-1}$.

**PART III: DO ANY THREE OF THESE FOUR PROBLEMS**

9. (20) The center $Z$ of a group $G$ is the set of all $z \in G$ with the property that $zg = zg$ for all $g \in G$. Prove that $Z$ is a subgroup of $G$. Prove that $Z$ is Abelian.

**Solution:** Three parts for the subgroup.
Identity: As \( eg = ge \) for all \( g \in G, \ e \in Z \).

Product: Assume \( x, y \in Z \). For all \( g \in G \)

\[
(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)
\]

so \( xy \in Z \).

Inverse: Assume \( x \in Z \). For any \( g \in G \) we have \( xg = gx \). Taking inverses, \( g^{-1}x^{-1} = x^{-1}g^{-1} \). Multiplying by \( g \) on the left and right

\( x^{-1}g = gx^{-1} \), so \( x^{-1} \in Z \).

Finally, we need Abelian. Let \( x, y \in Z \). We actually only need that \( x \in Z \) as that implies \( xy = yx \).

10. (20)

(a) (5) List the elements of \( Z_8^* \).
   Solution: \( 1, 3, 5, 7 \).

(b) (5) Give the multiplication table for \( Z_8^* \).
   Solution:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

(c) (10) Is \( Z_8^* \) isomorphic to \( (Z_4, +) \)? (Give your reason!)
   Solution: No. All elements of \( Z_8^* \) have order one (the identity) or two but in \( (Z_4, +) \) the element 1 has order four.

11. (20) Let \( G \) be an Abelian group under multiplication. Let \( x, y \in G \) with \( o(x) = p, o(y) = q \) where \( p, q \) are distinct primes. Prove that \( o(xy) = pq \).
   Solution: As \( (xy)^{pq} = x^{pq}y^{pq} = (x^p)^q(y^q)^p = e^q e^p = e \) the order of \( xy \) must divide \( pq \) and so must be \( 1, p, q \) or \( pq \). If it were one then \( xy = e \) so \( o(x) = o(y) \), which is not the case. If it were \( p \) then \( e = (xy)^p = x^py^p = ey^p \) so \( y^p = e \). As \( o(y) = q \) this would imply that \( q \) divided \( p \), but they are both primes and so this is not the case. Similarly it can’t be \( q \). So it must be \( pq \).

12. (20)

(a) (5) Define the terms Euclidean Domain and Principle Ideal Domain.
   Solution: A Euclidean Domain is an Integral Domain \( D \) with a size function \( d(\cdot) \) defined on the nonzero elements of \( D \) taking values in the nonnegative integers such that \( d(\alpha \beta) \geq d(\alpha) \) for all nonzero \( \alpha, \beta \) and, the critical division simulation, for all \( \alpha, \beta \) with \( \alpha \neq 0 \) there exist \( q, r \) with \( \beta = q\alpha + r \) and either \( r = 0 \) or \( d(r) < d(\alpha) \). A Principle Ideal Domain is one in which every ideal \( I \) can be written \( I = (\alpha) \) for some \( \alpha \).
(b) (15) Prove that a Euclidean Domain is a Principle Ideal Domain.

**Solution:** Let $I$ be an ideal. If $I = \{0\}$ then $I = (0)$. Otherwise let $\alpha$ be a nonzero element of $I$ with $d(\alpha)$ minimal. As $I$ is an ideal $(\alpha) \subseteq I$. Conversely, let $\beta \in I$. Find $q, r$ with $\beta = qa + r$ as above. If $r \neq 0$ we have $d(r) < d(\alpha)$ but $r = \beta - qa \in I$, contradicting the minimality of $d(\alpha)$. Thus $r = 0$ so $\beta \in (\alpha)$. That is, $I \subseteq (\alpha)$ and hence $I = (\alpha)$.
PART IV: NO PROOFS REQUIRED HERE

13. (5) Give an example of an integral domain \( D \) which is \textit{not} a field.
   \textbf{One Solution:} \( \mathbb{Z} \), the integers.

14. (5) Give an example of a finite group \( G \) which is \textit{not} Abelian.
   \textbf{One Solution:} \( S_3 \), the group of permutations on 3 symbols.

15. (5) Give an example of a ring \( R \) which is \textit{not} an Integral Domain.
   \textbf{One Solution:} \( \mathbb{Z}_6 \) as \( 2 \cdot 3 = 0 \).

16. (5) Give an example of a subgroup \( H \) of a group \( G \) where \( H \) is \textit{not} a normal subgroup.
   \textbf{One Solution:} Take \( G = S_3 \) and \( H = \{ e, \theta \} \) where \( \theta = (12) \), the transposition.

Problems will always torment us, because all important problems are insoluble: that is why they are important. The good comes from the continuing struggle to try to solve them, not from the vain hope of their solution.
Arthur Schlesinger, Jr. 1917-2007