Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in complete sentences. Your explanations are your only representative when your work is being graded.

Name: Ken Ribet

SID: Rough solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Max Points</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>

1. Find the smallest positive integer $n$ for which the alternating group $A_n$ has an element of order 1000.

Notice that $1000 = 10^3 = 2^35^3$. We can try to multiply an 8-cycle by a 125-cycle, but the 8-cycle will be odd and the 125-cycle will be even. I suspect that the best that we can do is to multiply together disjoint cycles of lengths 8, 2 and 125. My answer seems to be 135. I wonder if this is correct! I’ll find out soon enough when I grade the papers. If one can do better, surely a student will tell me how.

2. Show that every group of order 12 has a normal Sylow subgroup.

This is pretty standard, so maybe you’ve seen the problem before. The number of 3-Sylows divides 4 and is 1 mod 3. Therefore it’s either 1 or 4. If it’s 1, there’s a normal 3-Sylow. If not, there are $4 \times 2 = 8$ elements of order 3 in the group. This leaves four elements of order other than 3. The elements of a 2-Sylow (which has order 4) are of order $\neq 3$. Thus there can be only one 2-Sylow.
3. Let $R$ be an integral domain.

a. Explain what it means for an element of $R$ to be prime and what it means for an element of $R$ to be irreducible.

These notions are defined in the book.

b. Show that 2 is an irreducible element, but not a prime element, of the ring $\mathbb{Z}[\sqrt{-3}]$.

As I explained on a couple occasions in class, we have $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ in the ring. Clearly 2 cannot be prime because it divides neither factor on the right-hand side of the equation (but does divide their product, which is 4). On the other hand, 2 is irreducible because there is no element of norm 2 in the ring. (For details, see your class notes.)

c. Suppose that all ideals of $R$ are principal. If $r$ is an irreducible element of $R$, show that the ideal $(r)$ is maximal and that $r$ is a prime element of $R$.

If $r$ is irreducible and $I$ is an ideal of $R$ containing $(r)$, then $I = (a)$ for some $a \in R$. Because $r \in (r) \subseteq (a)$, $r$ is a multiple $ab$ of $a$. The equation $r = ab$ forces $a$ or $b$ to be a unit because $r$ is irreducible. In one case, $I = R$; in the other, $I = (r)$. Thus $(r)$ is a maximal ideal, which implies that it is a prime ideal. That $(r)$ is a prime ideal means that $r$ is a prime element, essentially by definition.

4. Let $A$ and $B$ be subsets of a finite group $G$ for which $|A| + |B| > |G|$. Let $g$ be an element of $G$, and let $gB^{-1} = \{ gb^{-1} \mid b \in B \}$. Show that $A \cap gB^{-1} \neq \emptyset$ and conclude that $g = ab$ for some $a \in A$, $b \in B$.


5. This problem concerns $n \times n$ matrices of real numbers.

a. Suppose that $M$ is such a matrix and that $X$ and $Y$ are $n \times n$ matrices with a single non-zero entry, which is equal to 1. Describe the product $XYM$ in terms of the entries of $M$ and the positions of the non-zero entries in $X$ and $Y$.

If $X$ has a “1” in position $ab$ and $Y$ has a “1” in position $cd$, then $XYM$ has $m_{bc}$ in position $ad$; all other entries in the product are 0. (I hope that this is correct!)

b. Show that the ring of $n \times n$ matrices of real numbers has no two-sided ideals other than $(0)$ and the whole ring.

Let $I$ be a 2-sided ideal of the indicated ring. Suppose $I$ is non-zero and let $M$ be a non-zero element of $I$. Say that the entry $m_{bc}$ is non-zero. Multiplying $M$ by an appropriate scalar matrix, we can and do assume that $m_{bc} = 1$. Then the various products $XYM$
have their unique 1’s in all possible positions \(ad\). By taking linear combinations of such products, we can get all elements of \(R\) inside \(I\).

6. Let \(C\) be a cyclic group of order \(p^n\), where \(p\) is an odd prime number and \(n\) is a positive integer. Show that \(C\) has a unique automorphism of order 2.

As we discussed in class numerous times, if \(C\) is cyclic of order \(N\), then the group of automorphisms of \(C\) is \((\mathbb{Z}/N\mathbb{Z})^\ast\). The problem is to show that \((\mathbb{Z}/p^n\mathbb{Z})^\ast\) has a unique element of order 2 (namely, \(-1\)). An element of order dividing 2 (i.e., of order 1 or 2) corresponds to an integer \(x\) satisfying \(x^2 \equiv 1 \pmod{p^n}\). Since, in particular, \(p\) will divide \(x^2 - 1 = (x - 1)(x + 1)\), we have \(x \equiv 1 \pmod{p}\) or \(x \equiv -1 \pmod{p}\). If \(x \equiv 1 \pmod{p}\), then \(p\) does not divide \(x + 1\). Hence the divisibility by \(p^n\) of the product \((x - 1)(x + 1)\) implies that \(p^n\) divides \(x - 1\), i.e., that \(x\) is 1 mod \(p^n\). In this case, the element of \((\mathbb{Z}/p^n\mathbb{Z})^\ast\) that we are dealing with is 1, which has order 1. If \(x \equiv -1 \pmod{p}\), then by an analogous argument we get \(x \equiv -1 \pmod{p^n}\). Of course, in this case the unique automorphism of order 2 of \(C\) is the map “inversion” or “multiplication by \(-1\),” depending on whether \(C\) is written multiplicatively or additively.

7. Suppose that \(I\) and \(J\) are ideals of a commutative ring \(R\) with the property that the canonical map

\[
R \rightarrow R/I \times R/J
\]

is surjective (“onto”). Show that \(I\) and \(J\) are comaximal in the sense that \(I + J = R\).

Take \(r \in R\) that maps to \((0, 1)\) under the canonical map. We have \(r + I = 0 + I\) and \(r + J = 1 + J\). The first equation means that \(r\) is an element of \(I\). The second means that \(1 - r\) is an element of \(J\), say \(s\). Then we have \(1 = r + s\) with \(r \in I\), \(s \in J\). It follows that the ideal \(I + J\) contains 1 and must therefore be all of \(R\).

8. Let \(n\) be a positive integer. Let \(R\) be the ring \(\mathbb{C}^n\) whose elements are \(n\)-tuples of complex numbers and whose ring operations are componentwise addition and multiplication. For each \(i\), \(1 \leq i \leq n\), let \(\pi_i : R \rightarrow \mathbb{C}\) be the \(i\)th projection \((x_1, \ldots, x_n) \mapsto x_i\).

a. Show that the kernel of \(\pi_i\) is a maximal ideal of \(R\).

By the first, isomorphism theorem, \(R/ \ker \pi_i\) is isomorphic to the image of \(\pi_i\). This image is clearly all of \(\mathbb{C}\), which is a field.

b. Prove that each maximal ideal of \(R\) is the kernel of \(\pi_i\) for some \(i\).

Let \(I\) be a maximal ideal of \(R\). Then \(I\) is a prime ideal. Also, \(I\) isn’t 0 because each of the \(\ker \pi_i\) in part (a) are proper ideals of \(R\) that are bigger than 0. In \(R = \mathbb{C}^n\), let \(e_1, \ldots, e_n\) be the “standard basis vectors” of linear algebra. For each pair of indices \(i\) and \(j\), we have \(e_i e_j = 0 \in I\). Hence for each pair \((i, j)\), either \(e_i\) or \(e_j\) is in \(I\). Since \(e_1 + \cdots + e_n = 1 \in R\), it is clear that \(I\) cannot contain all of the \(e_j\) (because \(I\) isn’t all of \(R\)). Let’s say specifically
that $e_i$ is not in $I$. Then, as explained above, all of the $e_j$ with $j \neq i$ are in $I$. By taking linear combinations of these elements, we see that $I$ contains all $(a_1, \ldots, a_n)$ with $a_i = 0$. But these elements constitute ker $\pi_i$! Hence $I$ contains ker $\pi_i$ and must be equal to ker $\pi_i$ because $I$ is proper and the kernel is maximal.