Bonus problem solutions 2

Problem. Let G be a group of order 56. Show that G is not simple.

Solution. Assume for the contrary that G is simple. This means that the number n_p of Sylow p-subgroups of G is greater than 1 for any p dividing 56. The factorization of 56 is

$$2^3 \cdot 7,$$

so we consider the Sylow 2-subgroups and Sylow 7-subgroups of G. The Sylow 2-subgroups have 8 elements, and Sylow 7-subgroups have 7 elements.

By the Third Sylow Theorem, we have $n_2|7$, so we must have $n_2 = 7$, since we are assuming $n_2 > 1$. Also by the Third Sylow Theorem, we have

$$n_7 \equiv 1 \pmod 7, \quad n_7|8.$$

This implies $n_7 = 8$, since we are assuming that $n_7 > 1$.

The Sylow 7-subgroups have order 7, which is prime, so the intersection of any two Sylow 7-subgroups is the trivial subgroup $\{1\}$. Thus, the union of all 8 Sylow 7-subgroups of G consists of $1 + 8 \cdot 6 = 49$ elements.

Thus, there are $56 - 49 = 7$ non-identity elements which are not contained in a Sylow 7-subgroup. Note that the intersection of any Sylow 2-subgroup with a Sylow 7-subgroup must also be the trivial subgroup $\{1\}$, since 8 and 7 are coprime. But this means that any Sylow 2-subgroup consists of 1 and the 7 remaining elements mentioned above.

So there can only be 1 Sylow 2-subgroup, contradicting the assertion that $n_2 = 7$.

Problem. Prove that every nonzero prime ideal of $\mathbb{Z}[\sqrt{-5}]$ is a maximal ideal.

Note: the original problem said $\mathbb{Z}[\sqrt{2}]$, which is a PID, and all nonzero prime ideals of any PID are maximal. But we do it here for $\mathbb{Z}[-5]$ instead, which is not a PID. The intention of the problem was to illustrate that this fact is also true for a more general class of rings. (But of course, there are rings in which not all nonzero prime ideals are maximal.)

Solution. Let I be a nonzero prime ideal of $\mathbb{Z}[\sqrt{-5}]$. Since it is nonzero, it contains some element

$$a + b\sqrt{-5}$$

for $a, b \in \mathbb{Z}$, with $(a, b) \neq (0, 0)$. By definition of ideal, I also contains the positive integer

$$n = (a + b\sqrt{-5}) \cdot (a - b\sqrt{-5}) = a^2 + 5b^2 > 0.$$

This means that $(n) \subseteq I$, which allows us to conclude that every element of $\mathbb{Z}[\sqrt{-5}]/I$ is equal to one of the n^2 cosets*

$$[r + s\sqrt{-5} + I], \quad r = 0, 1, 2, \ldots, n-1, \; s = 0, 1, 2, \ldots, n-1.$$

Thus, the quotient ring $\mathbb{Z}[\sqrt{-5}]/I$ has *at most* n^2 elements.

(Note that it could have less than n^2 elements; some of the n^2 cosets listed above could be equal.)

In any case, the key point is that we have shown that $\mathbb{Z}[\sqrt{-5}]/I$ has *finitely many* elements. Furthermore, since we assumed that I is a prime ideal, we know that $\mathbb{Z}[\sqrt{-5}]/I$ is an integral domain. By Problem 6 on Problem Set 7, a finite integral domain is a field, so $\mathbb{Z}[\sqrt{-5}]/I$ is actually a field! This is equivalent to saying that I is maximal.

***Remarks.**

- An alternative way of wording this is that every element of $\mathbb{Z}[-\sqrt{5}]$ is equivalent to one of the elements
$$r + s\sqrt{-5}, \quad 0 \leq r, s \leq n-1,$$
where $x, y \in \mathbb{Z}[\sqrt{-5}]$ are *equivalent* if $x - y \in I$.

- As an example, if $n = 6$, then
$$\overline{7 + 8\sqrt{-5}} = \overline{1 + 2\sqrt{-5}} \in \mathbb{Z}[\sqrt{-5}]/I,$$
since the difference of the two elements is
$$(7 + 8\sqrt{-5}) - (1 + 2\sqrt{-5}) = 6 + 6\sqrt{-5} \in (6) \subseteq \mathbb{Z}[\sqrt{-5}].$$
So we only need to count the element $\overline{1 + 2\sqrt{-5}}$ when counting elements in the quotient ring $\mathbb{Z}[\sqrt{-5}]/I$.

  (Here, $\overline{1 + 2\sqrt{-5}}$ is shorthand for the coset $[1 + 2\sqrt{-5} + I]$; it is just the image of the element $1 + 2\sqrt{-5}$ in the quotient ring. This is similar to how we denote elements of $\mathbb{Z}/n\mathbb{Z}$ by $\overline{a}$.)