Math 1530: Homework 5

Milan Capoor

24 October 2023

3.55

Let R be a ring, and let I be an ideal of R. In Exercise 3.49 you showed that there is a bijection

$$\{\text{ideals of R that contain I}\} \to \text{ideals of R/I}, \quad J \mapsto J/I$$

, *where J/I is the set of cosets*

$$J/I = \{a + I : a \in J\}.$$

Let J be an ideal of R that contains I.

1. *Prove that J is a prime ideal of R if and only if J/I is a prime ideal of R/I.*

   We will start by showing that if J is a prime ideal of R, J/I is a prime ideal of R/I.

   Let $a, b \in R$ with $ab \in J$. Then, by definition, $a \in J$ or $b \in J$. Assume WLOG that $a \in J$. We apply the bijection and $a + I \in J/I$. Now we take an element $r + I \in R/I$. By the formula for coset composition,

   $$(a + I)(r + I) = ar + I = 0 + I$$

   but since J is an ideal, by the absorber property $ar \in J$ so the product is in J/I. Thus J/I is prime.

   Now for the other direction, assume J/I is a prime ideal of R/I. Then with $a + I \in J/I$ and $r + I \in R/I$,

   $$(a + I)(r + I) = ar + I \in J/I$$

so $ar \in J$. But by the definition of J/I, we know that $a \in J$. So J is prime. ■

2. *Prove that J is a maximal ideal of R if and only if J/I is a maximal ideal of R/I.*

From the fact that J is in the set of ideals of R that contain I, we know that

$$I \subseteq J \subseteq R$$

Further, by the bijection $\pi(J) = J/I$ defined in exercise 3.49,

$$\pi(I) \subseteq \pi(J) \subseteq \pi(R)$$

This is well-defined because $R = (1)$ is an ideal of R which contains I (because I is an ideal of R) and similarly, I is an ideal of R which contains itself. By definition of the map, this is equal to

$$I/I \subseteq J/I \subseteq R/I$$

and $I/I = \{a + I : a \in I\} = I$.

So just from the definition of the bijection, we have that

$$I \subseteq J/I \subseteq R/I$$

If J/I is a maximal ideal of R/I, then we know there is no larger ideal in R/I which contains J/I. Further since the map described above is bijective, $\#J/I = \#J$ and $\#R/I = \#R$. Then looking at the preimage of the map, if J were not maximal, that would be mean that there is a larger ideal of R (an ideal of R which contained all of the elements of J plus more). But then the image of this larger ideal of R would have more elements than J/I so J/I could not be maximal and we have a contradiction. Thus, J must be maximal.

Similarly, if J is maximal, then we know that there is no larger ideal of R so the number of elements in J/I must be larger than the number of elements in any other ideal of R/I (except R/I itself). Thus, J/I is maximal. ■

5.3

Prove that each of the following subsets of $\mathbb{R}$ *is a field:*

Pursuant to Edstem post #120, we shall assume that all of the following sets are commutative rings. To show that they are fields thus amounts to showing that all non-zero elements have multiplicative inverses.

1. $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

   Let $a, b \neq 0$ and $a, b \in \mathbb{Q}$. Then,

   $$a + b\sqrt{3} \cdot \frac{1}{a + b\sqrt{3}} = 1$$

   and

   $$\begin{aligned} \frac{1}{a + b\sqrt{3}} &= \frac{1}{a + b\sqrt{3}} \cdot \frac{a - b\sqrt{3}}{a - b\sqrt{3}} \\ &= \frac{a - b\sqrt{3}}{a^2 - 3b^2} \\ &= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q} \quad \blacksquare \end{aligned}$$

2. $\mathbb{Q}(\sqrt{4}) = \{a + b\sqrt{4} : a, b \in \mathbb{Q}\}$.

   $\sqrt{4} = \pm 2$ so $\mathbb{Q}(\sqrt{4}) = \mathbb{Q}(\pm 2) = \mathbb{Q}(2)$ (because $\mathbb{Q}(-2)$ is just $\mathbb{Q}(2)$ with b^{-1} instead of b and since $\mathbb{Q}$ is a field, the inverses exist). Thus,

   $$\mathbb{Q}(\sqrt{4}) = \mathbb{Q}(2) = \{a + 2b : a, b \in \mathbb{Q}\}$$

   But since $2 \in \mathbb{Q}$ and it is closed under multiplication and addition, $a + 2b \in \mathbb{Q}$. As every element is in $\mathbb{Q}$, every element has an inverse, so it is a field. $\blacksquare$

3. $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

   We seek to find an element in $\mathbb{Q}[\sqrt[3]{2}]$ such that

   $$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = 1$$

   for $a, b, c, x, y, z \in \mathbb{Q}$.

   We can expand the product:

$$\begin{aligned}(a+b\sqrt[3]{2}+c\sqrt[3]{4})(x+y\sqrt[3]{2}+z\sqrt[3]{4}) &= ax+ay\sqrt[3]{2}+az\sqrt[3]{4}\\ &\quad+bx\sqrt[3]{2}+by\sqrt[3]{4}+2bz\\ &\quad+xc\sqrt[3]{4}+2yc+2cz\sqrt[3]{2}\\ &= ax+2cy+2bz+(ay+bx+2cz)\sqrt[3]{2}+(az+by+xc)\sqrt[3]{4}\end{aligned}$$

Since we want the product to be 1, we set the $\sqrt[3]{2}$ and $\sqrt[3]{4}$ terms to zero, which gives us a system of equations

$$\begin{aligned} ax+2cy+2bz &= 1\\ ay+bx+2cz &= 0\\ az+by+cx &= 0\end{aligned}$$

And we can represent this as a matrix equation:

$$\begin{pmatrix} a & 2c & 2b\\ b & a & 2c\\ c & b & a\end{pmatrix}\begin{pmatrix} x\\ y\\ z\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$

$$\begin{aligned}\begin{pmatrix} x\\ y\\ z\end{pmatrix} &= \frac{1}{a^3-6abc+2b^3+4c^3}\begin{pmatrix} a^2-2bc & 2b^2-2ac & -2ab+4c^2\\ 2c^2-ab & a^2-2bc & 2b^2-2ac\\ b^2-ac & 2c^2-ab & a^2-2bc\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}\\ &= \frac{1}{a^3-6abc+2b^3+4c^3}\begin{pmatrix} a^2-2bc\\ 2c^2-ab\\ b^2-ac\end{pmatrix}\end{aligned}$$

So the inverse of $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ is

$$\frac{a^2-2bc}{a^3-6abc+2b^3+4c^3}+\frac{2c^2-ab}{a^3-6abc+2b^3+4c^3}\sqrt[3]{2}+\frac{b^2-ac}{a^3-6abc+2b^3+4c^3}\sqrt[3]{4}$$

which is in $\mathbb{Q}[\sqrt[3]{2}]$. $\blacksquare$

5.4

Prove that each of the following rings is not a field:

1. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

   The inverse of $a + bi$ is

   $$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

   but $\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \notin \mathbb{Z}[i]$ so it is not a field. ■

2. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

   Similarly, the inverse of $a + b\sqrt{2}$ is

   $$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

   but $\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \notin \mathbb{Z}[\sqrt{2}]$ so it is not a field. ■

3. $\mathbb{Z}/p^2\mathbb{Z}$, where p is a prime.

   Consider $p = 2$. This leads to a contradiction because $\mathbb{Z}/4\mathbb{Z}$ is not a field:

   $$\begin{aligned} 2 \cdot 0 = 02 \cdot 1 &= 2 \\ 2 \cdot 2 &= 4 \\ 2 \cdot 3 &= 2 \end{aligned}$$

   So 2 does not have an inverse and thus not all rings $\mathbb{Z}/p^2\mathbb{Z}$ are fields. ■

4. $\mathbb{Z}/mn\mathbb{Z}$, where $m \geq 2$ and $n \geq 2$.

   Consider the case $m = 2, n = 3$. Then we have the “field” $\mathbb{Z}/6\mathbb{Z}$. But in this ring, the element 2 has no inverse:

   $$\begin{aligned} 2 \cdot 0 &= 0 \\ 2 \cdot 1 &= 2 \\ 2 \cdot 2 &= 4 \\ 2 \cdot 3 &= 0 \\ 2 \cdot 4 &= 2 \\ 2 \cdot 5 &= 4 \end{aligned}$$

So $\mathbb{Z}/6\mathbb{Z}$ is not a field. Having found a counterexample, we conclude $\mathbb{Z}/mn\mathbb{Z}$, where $m \geq 2$ and $n \geq 2$ is not always a field. ■

5.6a

Prove that

$$\sqrt{6} \notin S = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$$

and conclude that this set of real numbers is not a ring.

First notice that $\sqrt{6} \notin \mathbb{Q}$ so if it is in the set, it must be representable as a linear combination of $a, b\sqrt{2}, c\sqrt{3}$ with $a, b, c \in \mathbb{Q}$.

Then we consider the subfield $\mathbb{Q}[\sqrt{2}]$ of the set which corresponds to the linear combinations where $c = 0$. It is a field because for an element $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ (with $a, b \in \mathbb{Q}$),

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

Further, S is an abelian group under + because:

- Identity: $0 \in \mathbb{Q} \implies 0 \in S$
- Closure: by closure and distributivity of $\mathbb{Q}$,

  $$(a_1 + b_1\sqrt{2} + c_1\sqrt{3}) + (a_2 + b_2\sqrt{2} + c_2\sqrt{3}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} + (c_1 + c_2)\sqrt{3}$$

- Associativity: from closure and associativity of addition in $\mathbb{Q}$
- Inverses: Q is a field so $a^{-1} + b^{-1}\sqrt{2} + c^{-1}\sqrt{3} \in S$

Then since we have a field and an abelian group, we have a $\mathbb{Q}[\sqrt{2}]$-vector space. The proof of closure above also gives a sketch of the (trivial) proof that this vector space satisfies the axioms of vector composition.

This construction is helpful because it allows us to look at linear combinations in S. Consider $\{1, \sqrt{3}\}$ over $\mathbb{Q}[\sqrt{2}]$.

This set is linearly independent because

$$q_1 + q_2\sqrt{3} = 0 \implies q_1, q_2 = 0 \qquad (q_1, q_2 \in \mathbb{Q}\sqrt{2})$$

since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ so q_1 cannot be the additive inverse of $q_2\sqrt{3}$.

Further, the set of all linear combinations of $\{1, \sqrt{3}\}$ over $\mathbb{Q}[\sqrt{2}]$ is

$$\text{Span}\{1, \sqrt{3}\} = \underbrace{(a + b\sqrt{2})}_{\in\mathbb{Q}[\sqrt{2}]} + \underbrace{(c + d\sqrt{2})}_{\in\mathbb{Q}[\sqrt{2}]}\sqrt{3} = \underbrace{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}}_{a,b,c,d\in\mathbb{Q}} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

In other words, $\{1, \sqrt{3}\}$ is a $\mathbb{Q}[\sqrt{2}]$-basis for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

But we also have that $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}[\sqrt{2}]$ (Example 5.17). So this means that we have a tower of field extensions

$$\mathbb{Q}[\sqrt{3}, \sqrt{2}]/\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$$

By theorem 5.18, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ forms a $\mathbb{Q}$-basis for $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$.

Being a basis, we know that $\sqrt{6}$ can be written as the linear combination

$$\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

for exactly one set of scalars $a, b, c, d \in \mathbb{Q}$. Obviously, the choice of scalars is $a, b, c = 0, d = 1$, which means that $\sqrt{6}$ *cannot* be written as the sum $a + b\sqrt{2} + c\sqrt{3}$ for any choice of $a, b, c \in \mathbb{Q}$.

Hence, $\sqrt{6} \notin \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$ which was exactly what we were trying to show in the first place!

Finally, notice that $\sqrt{2}$ and $\sqrt{3}$ are both in the set but their product $\sqrt{6}$ is not. As the set is not closed under multiplication, it cannot be a ring. $\blacksquare$

5.7a

Let F be a finite field. Prove that

$$\prod_{a \in F^*} a = -1$$

Let p be a prime, and apply this formula to the field $\mathbb{F}_p$ to deduce Wilson's formula:

$$(p-1)! \equiv -1 \mod p.$$

(Hint. Which pairs of factors in the product cancel?)

As F is a field, the group of units $F^* = F \setminus \{0\}$. Then, since F is finite, the product over the group of units will be finite and nonzero. Further, every element which is not its own inverse will cancel. The only elements left are thus those which are there own inverse: $1, -1$. Both of these elements exist in every field because 1 is the multiplicative identity and -1 is the additive inverse of 1. Thus,

$$\prod_{a \in F^*} a = -1 \cdot 1 = -1$$

Now considering, $\mathbb{F}_p$, by Proposition 3.20, we have

$$\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots,\ p-1\}$$

Taking the product over the unit group and applying the formula, we get

$$\prod_{a \in \mathbb{F}_p^*} a = \prod_{i=1}^{p-1} i = 1 \cdot 2 \cdot \cdots \cdot p - 2 \cdot p - 1 = (p-1)! = -1 \quad \blacksquare$$