Solutions to Examination III Problems
Monday 24 November 2014

Problem 0.
Let m and n be positive integers. Let d be the greatest common divisor of m and n. Let ℓ be the least common multiple of m and n. Prove $mn = d\ell$.

Solution
Pick integers x and y so that

$$d = xm + yn$$

Then observe that

$$\ell d = xm\ell + yn\ell$$

We know that both m and n divide ℓ, since ℓ is a common multiple. So $mn \mid xm\ell$ and $mn \mid yn\ell$. In this way we see that $mn \mid \ell d$. This means that $\frac{mn}{d} \mid \ell$. But notice that

$$\frac{mn}{d} = \frac{m}{d}n = m\frac{n}{d}$$

Therefore $\frac{mn}{d}$ is a common multiple of m and n. But ℓ is the least (in the sense of the divisibility ordering) such common multiple. So $\ell \mid \frac{mn}{d}$. In this way we conclude that $\ell = \frac{mn}{d}$, or what is the same: $\ell d = mn$.

Problem 1.

Let A, B, and C be sets. Let h be a function from A onto B and let g be a function from A onto C. Let $\theta_h := \{\langle a, a'\rangle \mid a, a' \in A \text{ and } h(a) = h(a')\}$. Let $\theta_g := \{\langle a, a'\rangle \mid a, a' \in A \text{ and } g(a) = g(a')\}$. Suppose that there is a one-to-one function f from B onto C so that $f \circ h = g$.

Prove that $\theta_h = \theta_g$.

Solution
Just observe the following logical equivalences:

$$\begin{aligned}(a, a') \in \theta_h &\Leftrightarrow h(a) = h(a') \\ &\Leftrightarrow f(h(a)) = f(h(a')) \\ &\Leftrightarrow g(a) = g(a') \\ &\Leftrightarrow (a, a') \in \theta_g\end{aligned}$$

To get from the frist line to the second relies on the functionality of f while getting from the second line back to the first relies on the one-to-oneness of f. To get between the second and third lines uses $f \circ f = g$. The other equivalences use the definitions of θ_h and θ_g.

Problem 2 (Core).
Do each part below.

(a) Let $R = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$. Show that R is a subring of the ring $\mathbb{R}$ of real numbers.
(b) Let R be as defined in part (a) above. Define

$$F : R \to R$$

by $F(a + b\sqrt{5}) = a - b\sqrt{5}$ for all $a, b \in \mathbb{Z}$. Prove that F is a ring homomorphism.

SOLUTION
For part (a) we need to show that R is closed with respect to addition, multiplication, negation, and that it contains 0 and 1. I will only do one of these, closure with respect to multiplication, but the full solution needs all of these.

So suppose $a, b, c, d \in \mathbb{Z}$. Then

$$(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5}.$$

Since $ac + 5bd, ad + bc \in \mathbb{Z}$ we see that the product belongs to R.

For part (b) it is necessary prove that F respects all the basic ring operations. Again, I will only deal with multiplication, but the full solution must also contend with addition, negation, 0, and 1.

Just consider

$$\begin{aligned} F\big((a + b\sqrt{5})(c + d\sqrt{5})\big) &= F\big((ac + 5bd) + (ad + bc)\sqrt{5}\big) \\ &= (ac + 5bd) - (ad + bc)\sqrt{5} \\ &= (a - b\sqrt{5})(c - d\sqrt{5}) \\ &= F(a + b\sqrt{5})F(c + d\sqrt{5}) \end{aligned}$$

This shows that F respects multiplication.

PROBLEM 3 (Core).
Let $\mathbf{R}$ be a commutative ring. Prove that $\{r \mid r \in R \text{ and } r^n = 0 \text{ for some natural number } n\}$ is an ideal of $\mathbf{R}$.

SOLUTION
Let $I = \{r \mid r \in R \text{ and } r^n = 0 \text{ for some natural number } n\}$.

$0 \in I$
Well, notice that $0^1 = 0$ so we can use $n = 1$ to witness that $0 \in I$.

If $r, s \in I$, the $r + s \in I$
Suppose $r, s \in I$. Pick natural numbers n and m so that $r^n = 0$ and $s^m = 0$. What we need is a natural number k to witness that $r + s \in I$. That is we should come up with k so that $(r + s)^k = 0$. Remember the Binomial Theorem? Loosely, speaking it says that $(r + s)^k$ is a sum of terms that look like $r^i s^j$ where $i + j = k$. Example:

$$(r + s)^3 = r^3 s^0 + r^2 s^1 + r^2 s^1 + r^2 s^1 + r^1 s^2 + r^1 s^2 + r^1 s^2 + r^0 s^3.$$

Remember that we know that $r^n = 0$ and $s^m = 0$. So we want k so large that whenever $i + j = k$ then either $i \geq n$ or $j \geq m$. This will be true for $k = n + m$. That is $(r + s)^{(m+n)} = 0$. So $r + s \in I$.

If $r \in I$ and $t \in R$, then $tr \in I$
Suppose $r \in I$. Pick a natural number n so that $r^n = 0$. Then observe that $(tr)^n = t^n r^n = t^n 0 = 0$. So the natural number n testifies that $tr \in I$.

So I is an ideal.

PROBLEM 4.
Let $K = \{a + b\sqrt{8} \mid a, b \in \mathbb{Q}\}$, Prove that K is a field with respect to the usual ring operations on the real numbers.

SOLUTION
So conclude that K is a field, we must be convinced that K is a commutative ring in which $0 \neq 1$ and in which every nonzero element of K has a multiplicative inverse in K. Certainly, K is a subset of the real numbers, which we know to be a commutative ring in which $0 \neq 1$. So if we could show that K is closed with respect to the ring

operations we would know that K is also a commative ring in which $0 \neq 1$. I will only deal with multiplication, but a full solution must contend with all the operations.

For closure with respect to multiplication suppose $a, b, c, d \in \mathbb{Q}$. Then

$$(a + b\sqrt{8})(c + d\sqrt{8}) = (ac + 8bd) + (ad + bc)\sqrt{8}$$

and since $ac + 8bd, ad + bc \in \mathbb{Q}$, we see this product is back in K.

Now suppose that $a, b \in \mathbb{Q}$ and that $a + b\sqrt{8} \neq 0$. Because $\sqrt{8}$ is irrational, this can only happen when $a = 0 = b$. In this case $a - b\sqrt{8} \neq 0$ as well. Now observe

$$\frac{1}{a + b\sqrt{8}} = \frac{1}{a + b\sqrt{8}} \frac{a - b\sqrt{8}}{a - b\sqrt{8}} = \frac{a - \sqrt{8}}{a^2 - 8b^2} = \frac{a}{a^2 - 8b^2} + \frac{-b}{a^2 - 8b^2}\sqrt{8}.$$

It remains only to notice that $\frac{a}{a^2-8b^2}$ and $\frac{-b}{a^2-8b^2}$ are rational numbers.

Problem 5.

Let $\mathbf{R}$ be a commutative ring. Prove each of the following:

(a) Let M be an ideal of $\mathbf{R}$ and let $a \in R$ and let $J = \{c + ra \mid c \in M \text{ and } r \in R\}$. Prove that J is an ideal of $\mathbf{R}$.

(b) Suppose that M is an ideal of $\mathbf{R}$ so that if J is any ideal of $\mathbf{R}$ so that $M \subseteq J \subseteq R$, then $M = J$ or $J = R$. Prove that if $ab \in M$ and $a \notin M$, then $b \in M$.

Solution

For part (a), we see that $0 \in M$ since M is an ideal and $0 \in R$ as well. But $0 = 0 + 0a$ since we are in a ring. In this way, we see $0 \in J$. To see the J is closed with respect to addition, let $c, d \in M$ and $r, s \in R$. Then $c + ra$ and $d + sa$ are two arbitrary elements of J. Notice

$$(c + ra) + (d + sa) = (c + d) + (r + s)a,$$

where $c + d \in M$ since M is an ideal and $r + s \in R$ since R is closed with respect to addition. In this way, we see that J is closed under addition. Finally, to establishing the remaining property of ideals for J, let $c \in M$ and $r, s \in R$. Then

$$s(c + ra) = sc + (sr)a$$

and we know that $sc \in M$ since $c \in M$ and M is an ideal and also $sr \in R$. So J has the last property it needs to be an ideal.

For part (b), suppose M is a maximal proper ideal with $ab \in M$ and $a \notin M$. Let $J = \{c + ra \mid c \in M \text{ and } r \in R\}$. By part (a) J is an ideal. Evidently, $M \subseteq J$ since we can consistently choose $r = 0$ and let c run through M. On the other hand, $a \in J$ since we can let $c = 0$ and $r = 1$. We know that $a \notin M$. This means that $J = R$. Since $1 \in R$, we can pick $c \in M$ and $r \in R$ so that $1 = c + ra$. Multiplying both sides by b, we get

$$b = cb + rab.$$

But $c \in M$ so $cb \in M$ because M is an ideal. Also $ab \in M$ and so $rab \in M$. Finally because M is closed under addition, we get $cb + rab \in M$. But this means $b \in M$, just what we want.

PROBLEM 6.

Let D be a principal ideal domain and let a, b, and c be some fixed elements of D. Suppose that D is the only ideal of D that contains both a and b. Prove that if a divides bc, then a divides c.

SOLUTION

According to our supposition, $D = (a, b)$. We know that $(a, b) = \{ra + sb \mid r, s \in D\}$. This means we can pick $r, s \in D$ so that

$$1 = ra + sb.$$

Multiply both sides of this equation by c to obtain

$$c = rac + sbc.$$

Notice that $a \mid rac$ and $a|sbc$ since we are assuming a divides bc. As a consequence, a divides c as desired.

PROBLEM 7 (Core).

Let $3 \leq n$. Prove that there is no permutation $\sigma \in S_n$ such that $(0, 1, 2)\sigma^{-1}(0, 2) = \sigma$.

SOLUTION

We know that every 3-cylce is a product of two transpositions. Let us suppose that σ is a product of k transpositions. Then so is σ^{-1}. This means $(0, 1, 2)\sigma^{-1}(0, 2)$ is product of $k + 3$ transpositions, while σ is a product of k transpositions. But k and $k + 3$ have opposite parity: one is even and the other is odd. Since no permutation can be both even and odd is cannot happen that $(0, 1, 2)\sigma^{-1}(0, 2)$ and σ are equal.

PROBLEM 8 (Core).

Let $\mathbf{G}$ be a finite group and let $\mathbf{H}$ and $\mathbf{K}$ be subgroups of $\mathbf{G}$. Suppose that $[G : H]$ and $[G : K]$ are relatively prime. Prove that $[G : H][G : K]$ divides $[G : H \cap K]$.

SOLUTION

Because the two natural numbers $[G : H]$ and $[G : K]$ are relatively prime, we know that their product is also their least common multiple (least with respect to the ordering by divisibility). So to draw the desired conclusion, we need only show that the natural number $[G : H \cap K]$ is a common multiple of $[G : H]$ and $[G : K]$. That is we need to show the following divisibility relations:

$$[G : H] \mid [G : H \cap K] \text{ and}$$
$$[G : K] \mid [G : H \cap K]$$

Lagrange told us:

$$|G| = [G : H]|H|$$
$$|G| = [G : H \cap K]|H \cap K|$$
$$|H| = [H : H \cap K]|H \cap K|$$

From these it follows that $[G : H][H : H \cap K]|H \cap K| = [G : H \cap K]|H \cap K|$. Cancelling the $|H \cap K|$ from both sides we get

$$[G : H \cap K] = [G : H][H : H \cap K].$$

Using similar reasoning with K in place of H, we also get

$$[G : H \cap K] = [G : K][K : H \cap K].$$

In this way, we have the two divisibility conditions we need.

PROBLEM 9.
Let $\mathbf{G}$ and $\mathbf{H}$ be groups and suppose $F : G \to H$ satisfies that following property. $F(x^{-1}y) = F(x)^{-1}F(y)$ for all $x, y \in G$. Prove that F is a homomorphism from $\mathbf{G}$ into $\mathbf{H}$. [Advice: Can you determine $F(1)$?]

SOLUTION
We need to show that F respects the basic operations. Let us start by seeing that $F(1) = 1$.

Well, $1 = 1^{-1}1$, so $F(1) = F(1^{-1}1) = F(1)^{-1}F(1)$. But $\mathbf{H}$ is a group, so this last bit is just 1 (that is the 1 is $\mathbf{H}$.) So we see that $F(1) = 1$, as desired.

Now let's see about respecting inverses. $F(x^{-1}) = F(x^{-1}1) = F(x)^{-1}F(1) = F(x)^{-1}1 = F(x)^{-1}$. That's just what we want.

Finally, lets look at the product.

$$F(xy) = F\big((x^{-1})^{-1}y\big) = F(x^{-1})^{-1}F(y) = \big(F(x)^{-1}\big)^{-1}F(y) = F(x)F(y)$$

Bingo!

PROBLEM 10.
Let $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ be groups. Let h be a homomorphism from A onto B and let g be a homomorphism from A onto C. Define

$$f := \{\langle h(a), g(a)\rangle \mid a \in A\}.$$

Suppose further that f is a homomorphism from B into C.

Prove that $\ker h \subseteq \ker g$.

SOLUTION
Observe that $f \circ h = g$. To prove that $\ker h \subseteq \ker g$ we show that every element of $\ker h$ also belongs to $\ker g$. Just observe the following implications:

$$\begin{aligned} a \in \ker h &\Rightarrow h(a) = 1 \\ &\Rightarrow f(h(a)) = f(1) \\ &\Rightarrow f(h(a)) = 1 \\ &\Rightarrow g(a) = 1 \\ &\Rightarrow a \in \ker g. \end{aligned}$$

So $\ker h \subseteq \ker g$. This is just what we want.

PROBLEM 11.
Let $\mathbf{G}$ be a group and let H, K, and L be subgroups of $\mathbf{G}$ so that $H \subseteq L$. Prove that $HK \cap L \subseteq H(K \cap L)$.

SOLUTION
Suppose $a \in HK \cap L$. Then $a \in HK$ and $a \in L$. Pick $h \in H$ and $k \in K$ so that $a = hk$. Then $k = h^{-1}a$. Now $a \in L$ and $h^{-1} \in H \subseteq L$. So $ah^{-1} \in L$. This means $k \in L$. But of course, $k \in K$. So $k \in K \cap L$. That means that $a \in H(K \cap L)$ since $a = hk$ where $h \in H$ and $k \in K \cap L$. So we can conclude that $HK \cap L \subseteq H(K \cap L)$.
