Solutions Problem Set 0

Due Wednesday 27 August 2014

Problem 0.

For integers a and b we use (a, b) to denote the greatest common divisor of a and b. For example, $(12, 18) = 6$. In each part below find the greatest common divisor. [Hint: Try looking in some algebra textbook. . .]

a. $(6643, 2873)$.
b. $(26460, 12600)$.
c. $(12091, 8437)$.

Solution

The idea behind this is the use Euclid's algorithm based on the Key Fact about quotients and remainders. Here are the details for part (c):

$$\begin{aligned}
12091 &= 1 \cdot 8437 + 3654\\
8437 &= 2 \cdot 3654 + 1129\\
3654 &= 3 \cdot 1129 + 267\\
1129 &= 4 \cdot 267 + 61\\
267 &= 4 \cdot 61 + 23\\
61 &= 2 \cdot 23 + 15\\
23 &= 1 \cdot 15 + 8\\
15 &= 1 \cdot 8 + 7\\
8 &= 1 \cdot 7 + 1\\
7 &= 7 \cdot 1 + 0
\end{aligned}$$

showing that 1 is the greatest common divisor of 12091 and 8437.

Problem 1.

For each of the three parts of Problem 0, find integers m and n such that $(a, b) = ma + nb$.

Solution

The idea here is to run the Euclidean algorithm backwards, taking two steps, a replacement step and a rewrite step, for each step in the forward process. Here is part (c):

$$\begin{aligned}
1 &= 8 - 1 \cdot 7\\
&= 8 - 1(15 - 1 \cdot 8) = 2 \cdot 8 - 1 \cdot 15\\
&= 2(23 - 1 \cdot 15) - 1 \cdot 15 = 2 \cdot 23 - 3 \cdot 15\\
&= 2 \cdot 23 - 3(61 - 2 \cdot 23) = 8 \cdot 23 - 3 \cdot 61\\
&= 8(267 - 4 \cdot 61) - 3 \cdot 61 = 8 \cdot 267 - 35 \cdot 61\\
&= 8 \cdot 267 - 35(1129 - 4 \cdot 267) = 148 \cdot 267 - 35 \cdot 1129\\
&= 148(3654 - 3 \cdot 1129) - 35 \cdot 1129 = 148 \cdot 3654 - 479 \cdot 1129\\
&= 148 \cdot 3654 - 479(8437 - 2 \cdot 3654) = 1106 \cdot 3654 - 479 \cdot 8437\\
&= 1106(12091 - 1 \cdot 8437) - 479 \cdot 8437 = 1106 \cdot 12091 - 1585 \cdot 8437
\end{aligned}$$

$$\begin{aligned}
1 &= 8 - 1 \cdot 7\\
7 &= 15 - 1 \cdot 8\\
8 &= 23 - 1 \cdot 15\\
15 &= 61 - 2 \cdot 23\\
23 &= 267 - 4 \cdot 61\\
61 &= 1129 - 4 \cdot 267\\
267 &= 3654 - 3 \cdot 1129\\
1129 &= 8437 - 2 \cdot 3654\\
3654 &= 12091 - 1 \cdot 8437
\end{aligned}$$

So in this case $m = 1106$ and $n = -1585$.

Problem 2.

Give a proof of the properties of the divisibility relation listed in each part below.

a. For any integers a, b, and c, if $b \mid a$, then $b \mid ac$.

b. For any integers a, b, and c, if $b \mid a$ and $c \mid b$, then $c \mid a$.

Solution

For part (a), suppose $b \mid a$. Pick an integer k so that $a = bk$. Then $ac = (bk)c = b(kc)$, and we can conclude that $b \mid ac$ by the definition of divisibility.

For part (b), suppose $b \mid a$ and $c \mid b$. Use the definition of divisibility to pick integers k and n so that $a = bk$ and $b = cn$. From these two equations we deduce that $a = (cn)k = c(nk)$. According to the definition of divisibility, we conclude that $c \mid a$, as desired.

Problem 3.

Show that any nonempty set of integers that is closed under subtraction must also be closed under addition.

Solution

Let X be an nonempty set of integers that is closed under subtraction. Let $a, b \in X$. We need to show that $a + b \in X$. But $a + b = a - ((b - b) - b)$. Because $b \in X$ and X is closed under subtraction, then $b - b \in X$. Again by closure under subtraction, $(b - b) - b \in X$. One more application of closure under subtraction yields, $a - ((b - b) - b) \in X$. We never used that X is nonempty. Have we made a mistake, or is the empty set closed under addition as well?

Problem 4 (A Challenge Problem).

Which sets of natural numbers are closed under addition?

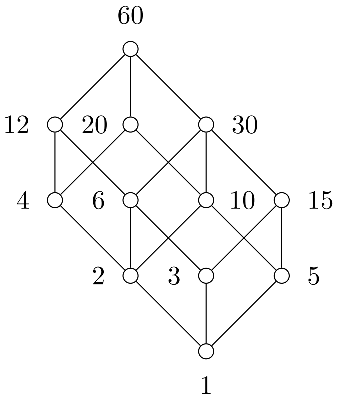
Solution

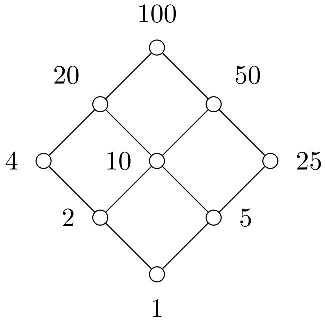
Keep working on this one!

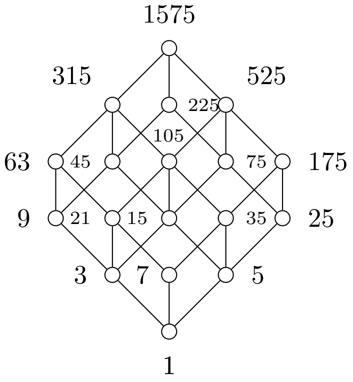
Solutions to Problem Set 1
Due 3 September 2014

Problem 5.
For each of the numbers $60, 100$, and 1575 draw the diagram of positive divisors showing the divisibility relation.

Solution







Problem 6.
Prove that $\frac{\log 2}{\log 3}$ is not a rational number.

Solution
Suppose, to the contrary, that $\frac{\log 2}{\log 3} = \frac{p}{q}$ where p and q are positive integers. So we see that $q \log 2 = p \log 3$. By the rules for manipulating logarithms, we get $\log(2^q) = \log 3^p$. As the logarithm function is one-to-one, we deduce that $2^q = 3^p$. Since q is a positive integer, we see that 2 divides 3^p. Since p is positive integer and 2 is prime, we find that 2 must divide 3, which is clearly wrong. So our supposition at the start was in error and $\frac{\log 2}{\log 3}$ cannot be rational.

Problem 7.
In each part below determine whether the function given is one-to-one, whether it is onto, and, in the event that it is both one-to-one and onto, describe its inverse.

(a) $f : \mathbb{R}^2 \to \mathbb{R}^2$ where $f(x, y) = (x + y, y)$.
(b) $f : \mathbb{R}^2 \to \mathbb{R}^2$ where $f(x, y) = (x + y, x + y)$.
(c) $f : \mathbb{R}^2 \to \mathbb{R}^2$ where $f(x, y) = (2x + y, x + y)$.

Solution
For part (a) the function is one-to-one and onto $\mathbb{R}^2$ and its inverse is the function $g : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $g(x, y) = (x-y, y)$. To see that just observe that $(f \circ g)(x, y) = f(g(x, y)) = f(x-y, y) = ((x-y)+y, y) = (x, y)$ and $(g \circ f)(x, y) = g(f(x, y)) = g(x + y, y) = ((x + y) - y, y) = (x, y)$. As every function with a two-sided inverse must be one-to-one and onto, our conclusion is secure.

For part (b), the function is neither one-to-one nor onto $\mathbb{R}^2$. The ontoness fails since for an output the two coordinates are identical. The means, for example, that the element $(0, 1)$ is never an output. One-to-oneness also fails, as witnessed by $f(1, 0) = (1, 1) = f(0, 1)$. So the distinct inputs $(1, 0)$ and $(0, 1)$ yield the same output.

For part (c), the function is both one-to-one and onto $\mathbb{R}^2$. Here is the inverse function: $g(x,y) = (x-y, 2y-x)$. Let's do it: $(f \circ g)(x,y) = f(g(x,y)) = f(x-y, 2y-x) = (2(x-y)+(2y-x), (x-y)+(2y-x)) = (x,y)$ and $(g \circ f)(x,y) = g(f(x,y)) = g(2x+y, x+y) = ((2x+y)-(x+y), 2(x+y)-(2x+y)) = (x,y)$.

PROBLEM 8.
Suppose that $f : A \to B$ and $g : B \to C$ and both f and g are one-to-one and onto. Prove that $(g \circ f)^{-1}$ is a function from C to A and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

SOLUTION
There are severl ways to approach this problem. The simplest depends on the fact that a function (here $g \circ f$) is one-to-one and onto if and only if it has a two-sided inverse. Since f and g are given as being one-to-one and onto they have inverses f^{-1} and g^{-1}. The idea is simply to devise a two-sided inverse for $f \circ g$ from these. It is even given in the problem: $f^{-1} \circ g^{-1}$. So lets just give it a try.

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ 1_B \circ f \\ &= f^{-1} \circ f \\ &= 1_A\end{aligned}$$

That was one side, here is the other.

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g \\ &= g \circ 1_B \circ g^{-1} \\ &= g \circ g^{-1} \\ &= 1_C\end{aligned}$$

Here I have used 1_A, 1_B, and 1_C to denote the identity functions on the sets A, B, and C.

Why is this a function from C to A? Well, g^{-1}, being the inverse of g, must be a one-to-one function from C onto B and f^{-1}, being the inverse of f, must be a one-to-one function from B onto A. So the composite function $f^{-1} \circ g^{-1}$ is a function from C to A.

PROBLEM 9 (Challenge Problem).
Prove that, for every positive naturaly number n, there are n consecutive composite natural numbers.

SOLUTION
Some teams submitted good solutions. If you still have this to do, keep working on it.

Solutions to Problem Set 2
Due 10 September 2014

Problem 10.

On the set $\mathbb{R}^2$ of ordered pairs of real numbers (think points in the plane) define the 2-place relation $\sim$ as follows:

$$(a,b) \sim (c,d) \text{ if and only if } a^2+b^2 = c^2+d^2.$$

(a) Prove that $\sim$ is an equivalence relation on $\mathbb{R}^2$.
(b) Describe the equivalence classes with respect to $\sim$.

Solution

For part (a), let us check the three defining properties of the notion of equivalence relation.

Relfexivity

$(a,b) \sim (a,b)$ holds for all choices of a and b since $a^2+b^2 = a^2+b^2$ holds for all such choices.

Symmetry

Suppose $(a,b) \sim (c,d)$. Then we know $a^2+b^2 = c^2+d^2$. This means, of course, that $c^2+d^2 = a^2+b^2$. Therefore, $(c,d) \sim (a,b)$, as desired.

Transitivity

This time we suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ and we hope to deduce that $(a,b) \sim (e,f)$. From the first relation, we get $a^2+b^2 = c^2+d^2$. From the second relation we get $c^2+d^2 = e^2+f^2$. Putting these equations together (using the transitivity of equality) we get $a^2+b^2 = e^2+f^2$, which allows us to draw the desired conclusion that $(a,b) \sim (e,f)$.

For part (b), we see that $\{(0,0)\}$, the set containing the origin, is one equivalence class. The others are just the cirles about the origin, with each radius giving us a distinct equivalence class. If we include that set containing the origin as its only point as a kind of trivial circle—a circle of radius 0—then we could say that the equivalence classes are exactly the circles about the origin.

Problem 11.

On the set $\mathbb{Z}$ of integers define the 2-place relation $\sim$ as follows:

$$m \sim n \text{ if and only if } n \mid m^k \text{ for some positive integer } k \text{ and } m \mid n^j \text{ for some positive integer } j.$$

(a) Prove that $\sim$ is an equivalence relation on $\mathbb{Z}$.
(b) Describe the equivalence class that contains 6 and describe the equivalence class that contains 12.
(c) Decribe the equivalence classes in general.

Solution

For part (a), let us check the three defining properties of the notion of equivalence relation.

Relfexivity

Let n be an integer. We see by definition that $n \sim n$ holds by taking $k = 1 = j$.

Symmetry

Suppose $n \sim m$ and that the positive integers k and j witness this. Then the postive integers j and k witness that $m \sim n$.

Transitivity

Suppose $n \sim m$ and $m \sim q$. Pick positive integers k, j, ℓ, and r so that $n \mid m^k, m \mid n^j, m \mid q^\ell$, and $q \mid m^r$. Observe that $n \mid m^k \mid (q^\ell)^k = q^{\ell k}$ and $q \mid m^r \mid (n^j)^r = n^{jn}$. So we conclude that $n \sim q$.

For part (b), we have $6 \sim m$ if and only if $6 \mid m^k$ for some positive integer k and $m \mid 6^j$ for some positive integer j. Now 2 is one of the prime factors of 6. So we see that $2 \mid m^k$. Since 2 is prime and k is a postive integer, we find that $2 \mid m$. Likewise $3 \mid m$. On the other hand, say p is a prime factor of m. Then $p \mid 6^j$. Since

p is prime and j is a positive integer, we see that $p \mid 6$. This means that the only 2 and 3 can be prime factors of m. What we see is that $6 \sim m$ if and only if the prime factors of m are exactly 2 and 3. So

$$\{m \mid 6 \sim m\} = \{2^\ell 3^q \mid \text{ where } \ell \text{ and } q \text{ are positive integers}\}.$$

In particular, $6 \sim 12$ so 6 and 12 have the same equivalence class.

For part (c), notice that the reasoning in part (b) is completely general. So $n \sim m$ if and only if n and m have exactly the same prime factors. There are two peculiar equivalence classes namely $\{0\}$ and $\{1\}$. The other equivalence class are associate with finite sets of primes in the following way. Let $p_0, p_1, \dots, p_{m-1}$ be m distinct primes. Then

$$\{p_0^{e_0} p_1^{e_1} \dots p_{m-1}^{e_{m-1}} \mid \text{ where } e_0, e_1, \dots, e_{m-1} \text{ are positive integers}\}$$

is an equivalence class and equivalence classes associated to distinct finite sets of primes are themselves distinct.

Problem 12.

Let X be a nonempty set and let $\sigma \in \operatorname{Sym} X$. Define the 2-place relation $\sim$ on X as follows:

$$x \sim y \text{ if and only if } \sigma^k(x) = y \text{ for some integer } k.$$

Prove that $\sim$ is an equivalence relation on X.

Solution

Let us check the three defining properties of the notion of equivalence relation.

Relfexivity

We see that $x \sim x$ if and only if $\sigma^k(x) = x$ for some k. Since σ^0 is the identity map, we see that $\sigma^0(x) = x$. Since 0 is an integer, with get $x \sim x$.

Symmetry

Suppose $x \sim y$. Pick an integer k so that $\sigma^k(x) = y$. Then $\sigma^{-k}(y) = x$. Since $-k$ is also an integer, we conclude that $y \sim x$.

Transitivity

Suppose that $x \sim y$ and $y \sim z$. Pick integers k and j so that $\sigma^k(x) = y$ and $\sigma^j(y) = z$. Then

$$\sigma^{j+k}(x) = \sigma^j(\sigma^k(x)) = \sigma^j(y) = z.$$

Since $j + k$ is an integer, we find that $x \sim z$.

Problem 13.

Let X be a nonempty set. Define the 2-place relation $\sim$ on $\operatorname{Sym} X$ as follows:

$$\sigma \sim \tau \text{ if and only if } \rho^{-1} \circ \sigma \circ \rho = \tau \text{ for some permutation } \rho.$$

Prove that $\sim$ is an equivalence relation on $\operatorname{Sym} X$.

Solution

Let us check the three defining properties of the notion of equivalence relation.

Relfexivity

We see that $\sigma \sim \sigma$ holds for all $\sigma \in \operatorname{Sym} X$ by taking ρ to the the identity permutation on X.

Symmetry

Suppose that $\sigma \sim \tau$. Pick $\rho \in \operatorname{Sym} X$ so that $\rho^{-1} \circ \sigma \circ \rho = \tau$. Observe,

$$\begin{aligned}
\sigma &= 1_X \circ \sigma \circ 1_X \\
&= (\rho \circ \rho^{-1}) \circ \sigma \circ (\rho \circ \rho^{-1}) \\
&= \rho \circ (\rho^{-1} \circ \sigma \circ \rho) \circ \rho^{-1} \\
&= \rho \circ \tau \circ \rho^{-1} \\
&= (\rho^{-1})^{-1} \circ \tau \rho^{-1}
\end{aligned}$$

So we see that the permutation ρ^{-1} witnesses that $\tau \sim \sigma$.

Transitivity

Suppose that $\sigma \sim \tau$ and $\tau \sim \eta$. Pick $\rho, \gamma \in \operatorname{Sym} X$ so that $\rho^{-1} \circ \sigma \circ \rho = \tau$ and $\gamma^{-1} \circ \tau\gamma = \eta$. Then we get

$$\begin{aligned}\eta &= \gamma^{-1} \circ (\rho^{-1} \circ \sigma \circ \rho) \circ \gamma \\ &= (\gamma^{-1} \circ \rho^{-1}) \circ \sigma \circ (\rho \circ \gamma) \\ &= (\rho \circ \gamma)^{-1} \circ \sigma \circ (\rho \circ \gamma)\end{aligned}$$

This means that the permutation $\rho \circ \gamma$ witnesses that $\sigma \sim \eta$.

Problem Set 3
Due 17 September 2014

Problem 14.
Prove that the inverse of any isomorphism is also an isomorphism.

Solution
Let F be an isomorphism between $\mathbf{A}$ and $\mathbf{B}$. So it is a homomorphism that is one-to-one and onto. Since F is one-to-one and onto we know that it has an inverse F^{-1} that is also one-to-one and onto. We only need to prove that F^{-1} is a homomorphism from $\mathbf{B}$ to $\mathbf{A}$. That is we have to show that F^{-1} preserves all the operations. So let $*$ be an operation of $\mathbf{B}$ and $\star$ be the corresponding operation of $\mathbf{A}$. I will suppose that these operations are 2-place operations (they must have the same number of inputs to correspond to each other) but the eager students will see that 2 could be replaced by any natural number. Pick b_0 and b_1 from B. Let $a_0 = F^{-1}(b_0)$ and $a_1 = F^{-1}(b_1)$. Now observe

$$\begin{aligned}
F^{-1}(b_0 * b_1) &= F^{-1]}\big(F(a_0) * F(a_1)\big)\\
&= F^{-1}\big(F(a_0 \star a_1)\big) \quad \text{since } F \text{ is a homomorphism}\\
&= a_0 \star a_1\\
&= F^{-1}(b_0) \star F^{-1}(b_1)
\end{aligned}$$

So F^{-1} must preserve all the operations. It is a homomorphism.

Problem 15.
Prove that the composition of two isomorphisms (if it is possible to form the composition) is also an isomorphism.

Solution
Suppose $\mathbf{A}, \mathbf{B}$, and $\mathbf{C}$ are algebraic systems with corresponding basis operations and that $F : \mathbf{A} \to \mathbf{B}$ and $G : \mathbf{B} \to \mathbf{C}$ are homomorphisms. We want to show that $G \circ F : \mathbf{A} \to \mathbf{C}$ is a homomorphism. We already know that $G \circ F$ is a function from A into C, so we only need to show it preserves all the basic operations. So let $*$ be a basic operation of $\mathbf{A}$ and let $\star$ and $\diamondsuit$ be the corresponding operations of $\mathbf{B}$ and $\mathbf{C}$ respectively. We suppose these are 2-place operations, but minor tweaking of the reasoning below shows that 2 can be replaced by any natural number. Let a_0 and a_1 be elements of A. Just observe

$$\begin{aligned}
(G \circ F)(a_0 * a_1) &= G\big(F(a_0 * a_1)\big)\\
&= G\big(F(a_0) \star F(a_1)\big)\\
&= G\big(F(a_0)\big) \diamondsuit G\big(F(a_1)\big)\\
&= (G \circ F)(a_0) \diamondsuit (G \circ F)(a_1)
\end{aligned}$$

This means $G \circ F$ preserves our (sample) basic operation. So it preserves all basic operations, making it a homomorphism.

Problem 16.
Let $\mathbf{R}$ be any ring. Prove that the following equations must hold in $\mathbf{R}$.

(a) $x \cdot 0 = 0$.
(b) $0 \cdot x = 0$.
(c) $-(-x) = x$.
(d) $(-x) \cdot (-y) = x \cdot y$.

Solution

Part (a) $x \cdot 0 = 0$

Observe $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. By what we know about group operations like $+$, we get $x \cdot 0 = 0$.

Part (c) $-(-x) = x$

From $-x + (-(-x) = 0$ we see $x + \big(-x + (-(-x))\big) = x + 0$. This gives $(x + (-x)) + (-(-x)) = x$. In turn we have $0 + (-(-x)) = x$ and finally $-(-x) = x$.

Part (d) $(-x) \cdot (-y) = x \cdot y$

First notice $0 = (-x) \cdot 0 = (-x) \cdot (y + (-y)) = (-x) \cdot y + (-x) \cdot (-y)$. Now observe

$$\begin{aligned}
x \cdot y &= x \cdot y + 0 \\
&= x \cdot y + \big((-x) \cdot y + (-x) \cdot (-y)\big) \\
&= \big(x \cdot y + (-x) \cdot y\big) + (-x) \cdot (-y) \\
&= \big(x + (-x)\big) \cdot y + (-x) \cdot (-y) \\
&= 0 \cdot y + (-x) \cdot (-y) \\
&= 0 + (-x) \cdot (-y) \\
&= (-x) \cdot (-y).
\end{aligned}$$

Problem 17.

Let I be any set and let R be the collection of all subsets of I. We impose on R the following operations:

$$\begin{aligned}
A + B &:= (A \cup B) \cap (\bar{A} \cup \bar{B}) \\
-A &:= A \\
0 &:= \emptyset \\
A \cdot B &:= A \cap B \\
1 &:= I
\end{aligned}$$

Here $\bar{A} = \{d \mid d \in I \text{ and } d \notin A\}$. The operation $+$ defined above is sometimes called the symmetric difference of the sets A and B. It may help to draw a Venn diagram of $A + B$. Prove that $\langle R, +, \cdot, -, 0, 1\rangle$, that is R equipped with the operaitons above, is a ring.

Solution

We will check that the algebraic system above is a commutative ring by demonstrating each of the equations that define the notion of commutative ring. This gets a bit thick, so the easier cases I will dismiss with minimalistic sketches.

We know that $\cap$ is associative and commutative from kindergarten. We also know $A \cap I = A$ since $A \subseteq I$.

Also notice that $A + B = (A \cup B) \cap (\bar{A} \cup \bar{B}) = (B \cup A) \cap (\bar{B} \cup \bar{A}) = B + A$, since $\cup$ has been commutative since kindergarten.

Next observe $A + A = (A \cup A) \cap (\bar{A} \cup \bar{A}) = A \cap \bar{A} = \emptyset = 0$. So A is the additive inverse of itself.

Before tackling the rest, let us recall the following equations that hold about $\cup, \cap$, and $\bar{\ }$.

$$\begin{aligned}
A\cap(B\cup C) &= (A\cap B)\cup(A\cap C)\\
A\cup(B\cap C) &= (A\cup B)\cap(A\cap C)\\
\bar{\bar{A}} &= A\\
\overline{(A\cup B)} &= \bar{A}\cap\bar{B}\\
\overline{(A\cap B)} &= \bar{A}\cap\bar{B}\\
A\cap(A\cup B) &= A\\
A\cup(A\cap B) &= A
\end{aligned}$$

This following equation is useful.

$$\begin{aligned}
A+B &= (A\cup B)\cap(\bar{A}\cup\bar{B})\\
&= \big((A\cup B)\cap\bar{A}\big)\cup\big((A\cup B)\cap\bar{B}\big)\\
&= \big((A\cap\bar{A})\cup(B\cap\bar{A})\big)\cup\big((A\cap\bar{B})\cup(B\cap\bar{B})\big)\\
&= (A\cap\bar{B})\cup(\bar{A}\cap B).
\end{aligned}$$

So $A+B=(A\cap\bar{B})\cup(\bar{A}\cap B)$.

Now consider the distributive law.

$$\begin{aligned}
A\cap(B+C) &= A\cap\big((B\cap\bar{C})\cup(\bar{B}\cap C)\big)\\
&= \big(A\cap B\cap\bar{C})\big)\cup\big(A\cap\bar{B}\cap C)\big)
\end{aligned}$$

On the other hand

$$\begin{aligned}
(A\cap B)+(A\cap C) &= \big((A\cap B)\cap\overline{(A\cap C)})\big)\cup\big(\overline{(A\cap\bar{B})}\cap(A\cap C)\big)\\
&= \big(A\cap B\cap(\bar{A}\cup\bar{C})\big)\cup\big((\bar{A}\cup\bar{B})\cap A\cap C\big)\\
&= \big((A\cap B)\cap\bar{A}\big)\cup(A\cap B\cap\bar{C})\cup\big((\bar{A}\cap A\cap C\big)\cup(\bar{B}\cap A\cap C)\\
&= \emptyset\cup(A\cap B\cap\bar{C})\cup\emptyset\cup(\bar{B}\cap A\cap C)\\
&= (A\cap B\cap\bar{C})\cup(A\cap\bar{B}\cap C)
\end{aligned}$$

So putting these together gives our distributive law

$$A\cap(B+C)=(A\cap B)+(A\cap C)$$

We still have to verify the associative law for $+$. Before tackling this it is handy to make the following deduction:

$$\begin{aligned}
\overline{A+B} &= \overline{(A\cup B)\cap(\bar{A}\cup\bar{B})}\\
&= \overline{(A\cup B)}\cup\overline{(\bar{A}\cup\bar{B})}\\
&= (\bar{A}\cap\bar{B})\cup(A\cap B)\\
&= \bar{A}+B
\end{aligned}$$

So we see $\overline{A+B}=\bar{A}+B$. Likewise, $\overline{A+B}=A+\bar{B}$.

Here is the associative law for $+$.

$$\begin{aligned}
A+(B+C) &= \big(A\cup(B+C)\big)\cap\big(\bar{A}\cup\overline{(B+C)}\big)\\
&= \big(A\cup(B+C)\big)\cap\big(\bar{A}\cup(\bar{B}+C)\big)\\
&= \Big(A\cup\big((B\cup C)\cap(\bar{B}\cup\bar{C})\big)\Big)\cap\Big(\bar{A}\cup\big((\bar{B}\cup C)\cap(B\cap\bar{C})\big)\Big)\\
&= \big((A\cup B\cup C)\cap(A\cup\bar{B}\cup\bar{C})\big)\cap\big((\bar{A}\cup\bar{B}\cup C)\cap(\bar{A}\cup B\cup\bar{C})\big)\\
&= (A\cup B\cup C)\cap(A\cup\bar{B}\cup\bar{C})\cap(\bar{A}\cup\bar{B}\cup C)\cap(\bar{A}\cup B\cup\bar{C})
\end{aligned}$$

On the other hand

$$\begin{aligned}(A+B)+C &= \big((A+B)\cup C\big)\cap\big(\overline{(A+B)}\cup\bar{C}\big)\\ &= \big((A+B)\cup C\big)\cap\big((\bar{A}+B)\cup\bar{C}\big)\\ &= \big(((A\cup B)\cap(\bar{A}\cup\bar{B}))\cup C\big)\cap\big(((\bar{A}\cup B)\cap(A\cup\bar{B}))\cup\bar{C}\big)\\ &= \big((A\cup B\cup C)\cap(\bar{A}\cup\bar{B}\cup C)\big)\cap\big((\bar{A}\cup B\cup\bar{C})\cap(A\cup\bar{B}\cup\bar{C})\big)\\ &= (A\cup B\cup C)\cap(\bar{A}\cup\bar{B}\cup C)\cap(\bar{A}\cup B\cup\bar{C})\cap(A\cup\bar{B}\cup\bar{C})\end{aligned}$$

In this way, we see that the associative law for $+$ holds. This completes our task.

Problem Set 4
Due 24 September 2014

Problem 18.
Let $\mathbf{R}$ and $\mathbf{S}$ be rings and let h and g be homomorphisms from $\mathbf{R}$ into $\mathbf{S}$. Let $T = \{r \mid r \in R \text{ and } h(r) = g(r)\}$. Prove that T is a subring of $\mathbf{R}$.

Solution
To see that T is a subring of $\mathbf{R}$ we demonstrate that it is closed under all the ring operations of $\mathbf{R}$.

$0 \in T$
$h(0) = 0 = g(0)$ since h and g are homomorphisms. So $0 \in T$.

$1 \in T$
$h(1) = 1 = g(1)$ since h and g are homomorphisms. So $1 \in T$.

If $r_0, r_1 \in T$, then $r_0 + r_1 \in T$
Suppose $r_0, r_1 \in T$. This means $h(r_0) = g(r_0)$ and $h(r_1) = g(r_1)$. From this we get $h(r_0) + h(r_1) = g(r_0) + g(r_1)$ buy adding the two equations together. But we know that h and g are homomorphisms, so we conclude $h(r_0 + r_1) = g(r_0 + r_1)$. Consequently, $r_0 + r_1 \in T$, as desired.

If $r_0, r_1 \in T$, then $r_0 \cdot r_1 \in T$
This works just like the argument just above, once $+$ is replaced everwhere by $\cdot$.

If $r \in T$, then $-r \in T$
Suppose $r \in T$. This means $h(r) = g(r)$. So $-h(r) = -g(r)$. But h and g are homomorphisms, so $-h(r) = h(-r)$ and $-g(r) = g(-r)$. Hence $h(-r) = g(-r)$. This means $-r \in T$, as desired.

Problem 19.
Let $R = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ and let $I = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z} \text{ and } m \text{ is even}\}$.

(a) Prove that $\mathbf{R}$ is a subring of the ring of real numbers.
(b) Prove that I is an ideal of $\mathbf{R}$.

Solution
For part (a) we need to show that R is closed under the ring operations on the real numbers.

$0 \in R$
Just notice $0 = 0 + 0\sqrt{2}$.

$1 \in R$
Just notice $1 = 1 + 0\sqrt{2}$.

If $r_0, r_1 \in R$, then $r_0 + r_1 \in R$
Pick integers a_0, b_0, a_1, and b_1 so that $r_0 = a_0 + b_0\sqrt{2}$ and $r_1 = a_1 + b_1\sqrt{2}$. Then $r_0 + r_1 = (a_0 + a_1) + (b_0 + b_1)\sqrt{2} \in R$.

If $r_0, r_1 \in R$, then $r_0 \cdot r_1 \in R$
Pick integers a_0, b_0, a_1, and b_1 so that $r_0 = a_0 + b_0\sqrt{2}$ and $r_1 = a_1 + b_1\sqrt{2}$. Then $r_0 \cdot r_1 = (a_0 \cdot a_1 + 2b_0 \cdot b_1) + (a_0 \cdot b_1 + a_1 \cdot b_0)\sqrt{2} \in R$.

If $r \in R$, then $-r \in R$
Pick integers a and b so that $r = a + b\sqrt{2}$. Then $-r = (-a) + (-b)\sqrt{2} \in R$.

For part (b), we need to check the definition of the concept of ideals.

$0 \in I$
Notice $0 = 0 + 0\sqrt{2}$ and that 0 is even.

If $a, b \in I$, then $a + b \in I$
Suppose $a, b \in I$. Pick even integers a_0, b_0, a_1, and b_1 so that $a = a_0 + a_1\sqrt{2}$ and $b = b_0 + b_1\sqrt{2}$. But then $a + b = (a_0 + b_0) + (a_1 + b_1)\sqrt{2}$. Since sums of even integers are even, we see $a + b \in I$, as desired.

If $a \in I$ and $r \in R$, then $ra, ar \in I$
Since $a \in I$, pick even integers a_0 and a_1 so that $a = a_0 + a_1\sqrt{2}$. Since $r \in R$, pick integers b and c so that $r = b + c\sqrt{2}$. But then $ar = ra = (a_0 b + 2a_1 c) + (a_0 c + b a_1)\sqrt{2}$. But observe that $a_0 b + 2a_1 c$ and $a_0 c_b a_1$ are both even, since a_0 and $2a_1 c$ are even. This means $ar = ra \in I$.

Problem 20.
Let $\mathbf{R}$ be the ring of all continuous functions from the set $\mathbb{R}$ of real numbers into $\mathbb{R}$ and let

$$I = \{f \mid f \in R \text{ and } f(\pi) = 0\}.$$

(a) Prove that I is a proper ideal of $\mathbf{R}$.
(b) Prove that if J is an ideal of $\mathbf{R}$ and $I \subseteq J \subseteq R$, then either $I = J$ or $J = R$.

Solution
For part (a) we need to check that the constantly 0 function belongs to I, that if $f, g \in I$, then $f + g \in I$, and that if $f \in I$ and $h \in R$, then $hf \in I$. These are very easy. Here is how to do the last one: Since $h(x)$ and $f(x)$ are continuous, we know from calculus that $h(x)f(x)$ is continuous. Also $h(\pi)g(\pi) = h(\pi) \cdot 0 = 0$. So $hg \in I$. We know I is a proper ideal since the constantly 1 function does not belong to I.

For part (a), Suppose that J is an ideal and $I \subseteq J$. In case $I = J$, we have one of the two alternative conclusions we desire. So suppose $I \neq J$. Let $f \in J$ with $f \notin I$. So f is continuous and $f(\pi) \neq 0$. Define $g(x) = 1 - \frac{1}{f(\pi)}f(x)$. This is possible since $f(\pi) \neq 0$. By calculus, $g(x)$ is continuous. Plainly, $g(\pi) = 0$. So $g \in I$. But this means $1 = g(x) + \frac{1}{f(\pi)}f(x)$. But $g \in I \subseteq J$. So we find $1 = g(x) + \frac{1}{f(\pi)}f(x) \in J$. Therefore $J = R$, the other alternative that we desire.

Problem 21.
Let $\mathbf{D}$ be a finite integral domain. Show that every nonzero element of D has a multiplicative inverse.

Solution
One property that characterizes finiteness of a set D is that every one-to-one function from D into D actually maps D onto D. Let us use this idea.

Let $u \in D$ with $u \neq 0$. We want to show that u has a multiplicative inverse v. This is the same as saying that the equation $1 - ux = 0$ has a solution v. So define $F : D \to D$ by $F(x) = 1 - ux$ for all $x \in D$.

We contend that F is one-to-one. To see this, suppose $F(a) = F(b)$. This means $1 - ua = 1 - ub$, which leads to $ua = ub$. But $u \neq 0$ and integral domains have the cancellation law. So we get $a = b$. In this way, we see that F is one-to-one. Since D is finite, F must map D onto D. So pick $v \in D$ so that $F(v) = 0$. This gives us $1 - uv = 0$. So $1 = uv$ and we find that v is a multiplicative inverse of u.

Solutions to Problems Set 5
Due 1 October 2014

Problem 22.
Let R be the ring of all continuous functions from the real numbers into the real numbers. Prove that R is not an integral domain.

Solution
This ring is easily seen to be commutative and in it 0 (that is the constantly 0 function) and 1 (that is the constantly 1 function) are distinct. To see it is not an integral domain we must devise two continuous functions f and g, neither constantly 0, whose product is constantly 0. Try these

$$f(x) = \begin{cases} x & \text{if } x > 0 \\ 0 & \text{if } x \leq 0 \end{cases}$$

$$g(x) = \begin{cases} 0 & \text{if } x > 0 \\ x & \text{if } x \leq 0 \end{cases}$$

Problem 23.
Let R be an integral domain and suppose that a is an element of R with the property that $a^2 = a$. Prove that either $a = 0$ or $a = 1$.

Solution
In integral domains we can cancel nonzero elements. So $a^2 = a = a \cdot 1$ implies either $a = 0$ or, by way of cancelling, $a = 1$.

Problem 24.
Let R be an integral domain and suppose that a and b are nonzero elements of R. Prove that

$$a \mid b \text{ and } b \mid a \Leftrightarrow b = au \text{ for some unit } u \in R.$$

Solution
First consider the $\Leftarrow$ direction. So $b = au$ where u is a unit. Becuase u is a unit there is v so that $uv = 1$. Now of course $b = au$ witnesses that $a \mid b$. On the other hand, $bv = auv = a \cdot 1 = a$, so $b \mid a$ as well.

Now consider the $\Rightarrow$ direction. So we suppose that $a \mid b$ and $b \mid a$ and we want to find a unit u so that $b = au$. First suppose that $a = 0$. Since $a \mid b$, this means that $b = 0$ as well. So $b = 0 = 0 \cdot 1 = a \cdot 1$ and we can let $u = 1$. So now suppose that $a \neq 0$. Then pick u so that $b = au$ and pick v so that $a = bv$. Then

$$a \cdot 1 = a = bv = (au)v = a(uv).$$

Since $a \neq 0$ we can cancel. This gives $1 = uv$. So u is a unit, as desired.

Problem 25.
Let R be an integral domain and let I and J be nontrivial ideals of R. Prove that $I \cap J$ is a nontrivial ideal of R.

Solution

First we verify that $I \cap J$ is an ideal.

$0 \in I \cap J$ since $0 \in I$ (because I is an ideal) and $0 \in J$ (because J is an ideal).

Suppose $a, b \in I \cap J$. The $a, b \in I$ and $ab, \in J$. So $a + b \in I$, since I is an ideal, and $a + b \in J$, since J is an ideal. Thus $a + b \in I \cap J$.

Now suppose $a \in I \cap J$ and $r \in R$. Then $a \in I$ and $a \in J$ since I and J. Then $ra \in I$ and $ra \in J$ since I and J are ideals. Thus, $ra \in I \cap J$.

So $I \cap J$ is an ideal.

We must show it is not trivial, knowing that I and J are not trivial. Pick $a \in I$ with $a \neq 0$ and pick $b \in J$ with $b \neq 0$. Then $ab \neq 0$ since R is an integral domain. Also $ab \in I$ and $ab \in J$ since I and J are ideal. So $ab \in I \cap J$. This means $I \cap J$ is nontrivial.

Problem Set 6
Due 8 October 2014

Problem 26.
Suppose that R is a commutative ring and that u is an element of R. Prove that u is a unit of R if and only if $u \mid r$ for all $r \in R$.

Solution
Suppose first that u is a unit. This means $u \mid 1$. Let r be any element of R. Since $r = 1 \cdot r$ we see that $1 \mid r$. Since $u \mid 1$ and the divisibility relation $\mid$ is transitive, we conclude that $u \mid r$.

Now suppose $u \mid r$ for all $r \in R$. Since 1 is an element of R, we see, in particular, that $u \mid 1$. This means u is a unit.

Problem 27.
Let R be an integral domain and suppose that $p \in R$ has the property that $p \neq 0$ and if $p \mid ab$, then either $p \mid a$ or $p \mid b$. Prove that p is irreducible. Bonus: show that $\mathbb{Z}_6$ does not have this property.

Solution
Suppose that $p = ab$. We must prove that either a is a unit or b is a unit. Since $p = ab$ we see that $p \mid ab$. So we have that $p \mid a$ or $p \mid b$. Consider the first alternative. Then we can pick r so that $a = pr$. This gives us $p = ab = prb$. Since $p \neq 0$ and since R is an integral domain, we can cancel p to get $1 = rb$. This means that b is a unit. For the other alternative, a very similar line of reasoning leads to the conclusion that a is a unit.

For the bonus, write out the multiplicatoin table of $\mathbb{Z}_6$. By examining this table you should be able to see that $2 = 2 \cdot 4 = 4 \cdot 5 = 2 \cdot 1$ and that up to commutativity these are the only ways to factor 2. Since the table also shows that $2 \mid 4$ and $2 \mid 2$, this means that 2 can play the role of p. However, since $2 = 2 \cdot 4$ and neither 2 nor 4 is a unit, we see that 2 fails to be irreducible.

Problem 28.
Prove that the ring $\mathbb{Z}_n$ is a field if and only if n is a prime number. Recall $\mathbb{Z}_n$ is the ring of remainders upon division by n where ring operations are defined modulo n.

Solution
Suppose first that n is not prime. Pick integers a and b so that $a > o < b$ and $ab = n$. Then $a, b \in \mathbb{Z}_n$ and neither $a = 0$ nor $b = 0$. but $a \cdot_n b = 0$. So the ring $\mathbb{Z}_n$ is not even an integral domain, much less a field.

Now suppose that n is prime. Let $a \in \mathbb{Z}_n$ with $a \neq 0$. We must show that a has a multiplicative inverse. We see that $0 < a < n$. So $n \nmid a$ because a is too small. Since n is prime its only postive factors are 1 and n. So 1 is the only common positive factor of n and a. This means n and a are relatively prime. So we can pick integers u and v so that

$$1 = nu + av.$$

Let b be the remainder of v upon division by n. Then the equation above tells us that $a \cdot_n b = 1$ and we have found the inverse of a.

Problem 29.
Let $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(1) Prove F is a subring of the field $\mathbb{R}$ of real numbers.
(2) Prove that F is a field.

Solution

A complete proof for part (a) consists of checking that F is closed under addition, multiplication, and negation, and that $0, 1 \in F$. I show here how to do multiplication and leave the rest to your attention.

So let $a_0, b_0, a_1, b_1 \in \mathbb{Q}$. Observe

$$(a_0 + b_0\sqrt{2})(a_1 + b_1\sqrt{2}) = (a_0a_1 + 2b_0b_1) + (a_0b_1 + a_1b_0)\sqrt{2}.$$

Since $a_0a_1 + 2b_0b_1$ and $a_0b_1 + a_1b_0$ are both rational, we see that the product of these two members of F belongs, itself, to F.

To prove part (b) it is only necessary to check that every nonzero element of F has a multiplicative inverse in F (since the other attributes of a field all follows from the fact that F is a subring of the field of real numbers). So let $a + b\sqrt{2} \neq 0$. Now just notice

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

Since $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are both rational, we see that $\frac{1}{a+b\sqrt{2}}$ belongs to F. (To really pull this off, you should also prove that $a - b\sqrt{2}$ is not 0. Can you do this??)

Solutions to Problem Set 7
Due 15 October 2014

Problem 30.
Write $(4,5,6)(5,6,7)(6,7,0)(0,1,2)(1,2,3)(3,4,5)$ as a product of disjoint cycles.

Solution

$$\begin{array}{ccccccccccccc}
 & & (4,5,6) & & (5,6,7) & & (6,7,0) & & (0,1,2) & & (1,2,3) & & (3,4,5) \\
1 & \longleftarrow & 1 & \longleftarrow & 1 & \longleftarrow & 1 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 0 \\
7 & \longleftarrow & 7 & \longleftarrow & 6 & \longleftarrow & 0 & \longleftarrow & 2 & \longleftarrow & 1 & \longleftarrow & 1 \\
3 & \longleftarrow & 3 & \longleftarrow & 3 & \longleftarrow & 3 & \longleftarrow & 3 & \longleftarrow & 2 & \longleftarrow & 2 \\
5 & \longleftarrow & 4 & \longleftarrow & 4 & \longleftarrow & 4 & \longleftarrow & 4 & \longleftarrow & 4 & \longleftarrow & 3 \\
4 & \longleftarrow & 6 & \longleftarrow & 5 & \longleftarrow & 5 & \longleftarrow & 5 & \longleftarrow & 5 & \longleftarrow & 4 \\
2 & \longleftarrow & 2 & \longleftarrow & 2 & \longleftarrow & 2 & \longleftarrow & 1 & \longleftarrow & 3 & \longleftarrow & 5 \\
6 & \longleftarrow & 5 & \longleftarrow & 7 & \longleftarrow & 6 & \longleftarrow & 6 & \longleftarrow & 6 & \longleftarrow & 6 \\
0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 7 & \longleftarrow & 7 & \longleftarrow & 7 & \longleftarrow & 7
\end{array}$$

So we get $(0,1,7)(2,3,5)$ as the disjoint cycle decomposition of our permutation. Notice, that this permutation fixes both 4 and 6.

Problem 31.
Let X be a set and $a \in X$. A permutation $\sigma \in \operatorname{Sym} X$ is said to **fix** a provided $\sigma(a) = a$. Let H be the collection of all permutations of X that fix the element a. Prove each of the following:

(a) $\mathbf{1}_X \in H$, where $\mathbf{1}_X$ is the identity function on X.
(b) If $\sigma \in H$, then $\sigma^{-1} \in H$.
(c) If $\sigma, \tau \in H$, then $\sigma \circ \tau \in H$.

Solution
We see part (a), since the identity permutation 1_X fixes each element of X, so in particular, it fixes a. So $1_X \in H$.

For part (b), suppose that $\sigma \in H$. So $\sigma(a) = a$. But then

$$a = 1_X(a) = (\sigma^{-1} \circ \sigma)(a) = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a).$$

So σ^{-1} also fixes a. This means $\sigma^{-1} \in H$.

For part (c), suppose $\sigma, \tau \in H$. This means both σ and τ fix a. But then

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a.$$

So we see that $\sigma \circ \tau$ fixes a. This means $\sigma \circ \tau \in H$.

Problem 32.
Let S_n be the set of all permutations of the set $\{0, 1, 2, \ldots, n-1\}$. Suppose that $n \geq 3$. Prove that every even permutation in S_n can be written as a product of cycles of length 3.

Solution
An even permutation has the form

$$(a_0, b_0)(a_1, b_1) \ldots (a_{2k}, b_{2k})(a_{2k+1}, b_{2k+1})$$

for some natural number k, where $a_i \neq b_i$ for all $i \leq 2k+1$. Consider the first two transpositions $(a_0, b_0)(a_1, b_1)$. There are three cases to consider:

Case: $\{a_0, b_0\}$ and $\{a_1, b_1\}$ have no elements in common
Let us try to write $(a_0, b_0)(a_1, b_1)$ as a product of 3-cylces. Our first attempt is to use two 3-cycles. We imagine

$$(a_0, b_0)(a_1, b_1) = (x, y, z)(a_0, b_0, w)$$

see at least that a_0 gets sent to b_0 by the 3-cycle on the right. We hope to determine the unknowns $x, y, z,$ and w in such a way that b_0 does not occur among $x, y,$ and z. The 3-cycle on the right sends b_0 to w so the 3-cycle on the left must send w to a_0. Plugging this in we get

$$(a_0, b_0)(a_1, b_1) = (w, a_0, z)(a_0, b_0, w).$$

So far so good. Now of course w should be one of a_1 or b_1 and it shouldn't matter which, say $w = a_1$. So we can have

$$(a_0, b_0)(a_1, b_1) = (a_1, a_0, z)(a_0, b_0, a_1).$$

Now consider what should happen to a_1. The 3-cycle on the right sends a_1 to a_0 and the 3-cycle on the left sends a_0 to z. So z must be b_1, which is where a_1 must ultimately wind up. But we need to check that b_1 also gets sent to a_1. Can you do this? In the end, we have

$$(a_0, b_0)(a_1, b_1) = (a_1, a_0, b_1)(a_0, b_0, a_1).$$

In this case, we see that the product of two transpositions can the replaced by the product of two 3-cycles.
Case: $\{a_0, b_0\}$ and $\{a_1, b_1\}$ have exactly one element in common
Let us say, without loss of generality, that $a_0 = a_1$. Then an easy computation shows

$$(a_0, b_0)(a_0, b_1) = (a_0, b_1, b_0).$$

So the product of two transposition that share exact one element turns out to be a 3-cylce.
Case: $\{a_0, b_0\} = \{a_1, b_1\}$
In this case the two transpositions are identical and their product is just the identity permutation. Since the identity permutation is a product of 0 3-cycles, we are okay here too.

Now just take our arbitrary even permutation, write it as a product of an even number of transpositions. Group this product in little packets of two transpositions each:

$$\big((a_0, b_0)\big)\big((a_1, b_1)(a_2, b_2)(a_3, b_3)\big)\ldots\big((a_{2k}, b_{2k})(a_{2k+1}, b_{2k+1})\big)$$

and then replace each packet with a product of 3-cycles. This gives a product of 3-cycles.

Problem 33.
Show that every permutation of the set $\{0, 1, 2, \ldots, n-1\}$ can be represented as a product, maybe a long one, using only the following $n-1$ transpositions

$$(0, 1), (0, 2), \ldots, \text{ and } (0, n-1).$$

Solution
Since we already know that every permutation can be written as a product of transpositions, it will be enough for us the show that each transposition can the written as a product of the particular transposition given in the list above.

So let us try to make the transposition $(1, 2)$. A little bit of fiddling shows that $(1, 2) = (0, 1)(0, 2)(0, 1)$. How about the more general case when $a, b < n$ and $a \neq b$. Can be make (a, b). Let's just try what worked with $(1, 2)$. Namely, try $(0, a)(0, b)(0, a)$. This works, as you can easily see.

So we see that we can obtain arbitrary transpositions by taking products, with just three factors, of the transpositions on our given list. This means we can write every permutation as a product of transpositions from our given list.

Problem 34 (Challenge Problem).

Prove that every permutation of $\{0, 1, 2, \ldots, 6\}$ can be written as a product, maybe a long one, built up using just the transposition $(0, 1)$ and the 7 cycle $(0, 1, 2, \ldots, 6)$. Is this still true if our 7-element set is replaced by one with 6-elements? What about 5-elements? What values of n work?

Solution

A hint: Figure out $(0, 1, 2, 3, 4, 5, 6)(0, 1)(6, 5, 4, 3, 2, 1, 0)$. Then figure out $(1, 2)(0, 1)(1, 2)$.

Problem Set 8
Due 22 October 2014

Problem 35.

Prove that $\sigma\tau\sigma^{-1}\tau^{-1} \in A_n$, for any $\sigma, \tau \in S_n$.

Solution

We know that every permutation in S_n can be expressed as a product of transpositions. So suppose σ can be expressed as a product of k transpositions and τ can be expressed as a product of n transpositions. Now recalling that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ and that every transposition is its own inverse, we see that σ^{-1} can be expressed as the product of k transpositions and τ^{-1} as the product of n transpositons. Putting this together, we have that $\sigma\tau\sigma^{-1}\tau^{-1}$ can be expressed as a product of $k+n+k+n = 2(k+n)$ transpositions. This means that $\sigma\tau\sigma^{-1}\tau^{-1}$ can be expressed as a product of an even number of transpositions. This puts it into A_n.

Problem 36.

Without writing down all 60 elements of $\mathbf{A}_5$ (the group of all even permutations on a five-element set), describe the possible shapes of the permutations (the number and length of their disjoint cycles) and how many of each type there are.

Solution

Let us begin by figuring out which cycles are even and which are odd. Recall the proof that every permutation on a finite set can be written as a product of transpositions. That proof actually showed us how to express a cycle of length n as a product on $n-1$ transpositions. This means that cycles of even length are odd and those of odd length are even.

Consider $\sigma \in S_5$. Express it as a product of dijoint cycles. What are the possibilities and which of them belong to A_5?

Cycle Structure	Even or Odd?
the identity map	Even
(a,b)	Odd
$(a,b)(c,d)$	Even
(a,b,c)	Even
$(a,b,c)(d,e)$	Odd
(a,b,c,d)	Odd
(a,b,c,d,e)	Even

Now lets do some counting.

There is only 1 identity map.

Consider $(a,b)(c,d)$. There are 5 choices for a. There are 4 remaining choices for b. There are 3 choices remaining for c. And then 2 for d. So it looks like 5!. But wait. $(a,b) = (b,a)$ and $(c,d) = (d,c)$ so we counted some things too many times. Now it looks like we should have $\frac{5!}{2\cdot 2}$. But wait once more! $(a,b)(c,d) = (c,d)(a,b)$. So it should be $\frac{5!}{2\cdot 2\cdot 2} = 15$.

Consider (a,b,c). There are 5 choices for a, then 4 for b, and finally 3 for c. This gives $\frac{5!}{(5-3)!}$. But wait. $(a,b,c) = (b,c,a) = (c,a,b)$ so we over counted again. It should be $\frac{5!}{(5-3)!3} = 20$.

Consider, finally, (a,b,c,d,e). Reasoning as with the case above, we get $\frac{5!}{(5-5)!5} = 24$.

So in A_5 we have 1 permutation, namely the identity, with an empty cycle structure. We have 15 permutations that are the product of two disjoint transpositions. We have 20 permutaitons that are 3-cycles. We have 24 permutations that are 5-cycles. That is altogether 60 even permutations.

This is nice. We know that the number of permutations of 5 things is $5! = 120$. So we see that A_5 contains exaclty half the elements of S_5. Does this hold for numbers different from 5?

Problem 37.

Let X be an infinite set. Let H be the set of all elements σ of $\operatorname{Sym} X$ such that $\sigma(x) = x$ for all but finitely many $x \in X$. Prove that H is subgroup of $\operatorname{Sym} X$.

Solution

What we must show is that H is closed under the group operations. That means we have to check 3 things.

Is 1_X a member of H?

Sure. The identity fixes every element. So the set of elements moved by the identity is empty. The empty set is finite.

If $\sigma \in H$, then is $\sigma^{-1} \in H$?

Well, let $M = \{x \mid x \in X \text{ and } \sigma(x) \neq x\}$. This is the set of elements moved by σ. Our hypothesis is that M is finite. Now suppose that $\sigma^{-1}(y) = z$ and that $y \neq z$. It is impossible that $\sigma(y) = y$ since this would give $y = \sigma^{-1}(\sigma(y)) = \sigma^{-1}(y) = z$. So if y is moved by σ^{-1}, then y is moved by σ. This puts every element moved by σ^{-1} into M. But M is finite, so σ^{-1} can move on finitely many points.

If $\sigma, \tau \in H$, then is $\sigma \circ \tau \in H$?

. Let M be the set of points moved by σ and N be the set of points moved by τ. Now it is easy to see that if x is fixed by *both* σ and τ, then it must be fixed by $\sigma \circ \tau$:

$$(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x.$$

So this means that every point moved by $\sigma \circ \tau$ must be moved by either σ or by τ or by both. Hence, every point moved by $\sigma \circ \tau$ mut belong the $M \cup N$. Because the union of two finite sets must be finite, we see that $\sigma \circ \tau$ can move only finitely many points. So $\sigma \circ \tau \in H$, as desired.

Problem 38 (Challenge Problem).

Prove that every group with n elements is isomorphic to a subgroup of the group of all invertible linear operators on the n-dimensional real vector space. Would something like this remain true if n were infinite? Would that even mean anything?

Problem Set 9
Due 29 October 2014

Problem 39.

Let n, a, and b be positive integers. Suppose that n and a are relatively prime and that $n \mid ab$. Prove that $n \mid b$.

Solution

Because n and a are relatively prime we can pick integers u and v so that $1 = un + va$. Multiply both sides by b to get $b = unb + vab$. Since $n \mid ab$, we also pick an integer w so that $ab = wn$. But then

$$b = unb + vab = unb + vwn = (ub + vw)n.$$

So $n \mid b$.

Problem 40.

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 $\theta_g := \{\langle a, a'\rangle \mid a, a' \in A \text{ and } g(a) = g(a')\}$. Define

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

Suppose further that f is a one-to-one function from B into C.

Prove that $\theta_h = \theta_g$.

Solution

To prove that two sets are equal we argue that they have the same elements. In our particular case we want the show that $\theta_h = \theta_g$. Here is one way.

$$\begin{aligned}\langle a, a'\rangle \in \theta_h &\text{ if and only if } h(a) = h(a')\\ &\text{ if and only if } f(h(a)) = f(h(a'))\\ &\text{ if and only if } g(a) = g(a')\\ &\text{ if and only if } \langle a, a'\rangle \in \theta_g.\end{aligned}$$

The first logical equivalence is just the definition of θ_h. For the second logical equivalence the downward direction follows from applying the function f to both sides, while the upward direction follows from the one-to-oneness of f. The third equivalence just uses the definition of f. The last equivalence uses the definition of θ_g.

Problem 41.

Let $\mathbf{G}$ be a group and let $\mathbf{H}$ be a subgroup of $\mathbf{G}$. Let

$$N = \{g \mid g \in G \text{ such that } x^{-1}gx \in H \text{ for all } x \in G\}.$$

Prove that N is a subuniverse of $\mathbf{G}$.

Solution

What is needed is to show that the set N is closed under the basic operations of $\mathbf{G}$.

First, $1 \in N$, since $x^{-1} \cdot 1 \cdot x = x^{-1}x = 1$ for all $x \in G$ and we know that $1 \in H$, since $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

Next, suppose $g \in N$ and x is an arbitrary element of G. So it must be that $x^{-1}gx \in H$, by the definition of N. But $(x^{-1}gx)^{-1} = x^{-1}g^{-1}x$. Since $\mathbf{H}$ is a subgroup of $\mathbf{G}$, we see that H is closed under formation of inverses. So $x^{-1}g^{-1}x \in H$. Since this is true for arbitrary elements $x \in G$, we see that $g^{-1} \in N$, as desired.

Last, suppose $g_0, g_1 \in N$. We want to show that $g_0g_1 \in N$. So let x be any element of G. Then $x^{-1}g_0g_1x = x^{-1}g_0xx^{-1}g_1x$. Now we know that $x^{-1}g_0x \in H$ and $x^{-1}g_1x \in H$, since that is what put g_0 and g_1 into N.

Morever we know that H is closed under the product, since $\mathbf{H}$ is a subgroup of $\mathbf{G}$. In this way, we find that $x^{-1}(g_0g_1)x \in H$. But this entails that $g_0g_1 \in N$, as desired.

Problem 42.

Problem 3

Let n and k be positive integers and h be a homomorphism from $\langle \mathbb{Z}_n, +_n, \cdot_n, -_n, 0, 1\rangle$ onto $\langle \mathbb{Z}_k, +_k, \cdot_k, -_k, 0, 1\rangle$. Prove each of the following statements.

a. $k \leq n$.
b. $h(k) = 0$. [Hint: $h(1 +_n \cdots +_n 1) = h(1) +_k \cdots +_k h(1)$.]
c. $h(a) = r$ for each $a \in \{0, 1, \ldots, n-1\}$, where $a = kq + r$ with $r \in \{0, 1, \ldots, k-1\}$ for some integer q.
d. $k \mid n$.

Solution

We know that $(0,1,2)$ is an even permutation and that $(0,2)$ is an odd permutation. Now σ must be either even or odd, since every permutation can be expressed as a product of transpositions. If σ is even then $(0,1,2)\sigma$ is even and $\sigma(0,2)$ is odd. Since no permutation is both even and odd, we must reject $(0,1,2)\sigma = \sigma(0,2)$ in this case. The other alternative is that σ is odd. In this case, $(0,1,2)\sigma$ is odd and $\sigma(0,2)$ is even, so we must also reject $(0,1,2)\sigma = \sigma(0,2)$ in this case. So there is no permutation σ so that $(0,1,2)\sigma = \sigma(0,2)$.

Problem Set 10
Due 5 November 2014

Problem 43.
By $\mathbb{Z}_2$ we mean the algebra $\langle\{0,1\},\oplus,\ominus,0\rangle$ where the two place operation $\oplus$ is given by

$$0\oplus 0=0 \qquad 1\oplus 1=0$$
$$0\oplus 1=1 \qquad 1\oplus 0=1$$

and $\ominus$ works so that $\ominus 0=0$ and $\ominus 1=1$. With these operations $\mathbb{Z}_2$ is a group (and eager students will check this). Now let $n>2$ be a natural number and let h be the map from S_n to $\{0,1\}$ defined so that $h(\sigma)=0$ if σ is an even permutation and $h(\sigma)=1$ if σ is an odd permutation. Prove that h is a homomorphism from $\mathbf{S}_n$ onto $\mathbb{Z}_2$. Also discover what the kernel of h is.

Solution
Actually, $\mathbb{Z}_2$ is isomorphic to $\mathbf{S}_2$, as the eager students can verify.

Since we know that $\mathbf{S}_n$ and $\mathbb{Z}_2$ are both groups, to check that h is a homomorphism all we need to do is prove

$$h(\sigma\circ\tau)=h(\sigma)\oplus h(\tau)$$

for all $\sigma,\tau\in S_n$. Suppose first that σ is an even permutation. Then $h(\sigma)=0$ and $\sigma\circ\tau$ is even or odd depending only on whether τ is even or odd. In this case, we have

$$h(\sigma\circ\tau)=h(\tau)=0\oplus h(\tau)=h(\sigma)\oplus h(\tau),$$

So in the case that σ is even we get the desired conclusion.

Suppose, on the other hand, that σ is an odd permutation. Then $h(\sigma)=1$ and $\sigma\circ\tau$ has the opposite parity of τ. Because of the way that $\oplus$ is defined, this last means that $h(\sigma\circ\tau)=1\oplus h(\tau)$. But then we see

$$h(\sigma\circ\tau)=1\oplus h(\tau)=h(\sigma)\oplus h(\tau),$$

which is just what we need.

The kernel of h is the set $\{\sigma\mid h(\sigma)=0\}=\{\sigma\mid \sigma \text{ is an even permutation}\}=A_n$. In this way, we see that $\mathbf{A}_n$ is a normal subgroup of $\mathbf{S}_n$.

Problem 44.
Let $\mathbb{C}^\times$ be the group of nonzero complex numbers, where the two place operation is complex multiplication, the one-place operation is multiplicative inverse, and the identity is 1. Likewise, let $\mathbb{R}^+$ be the group of positive real numbers with the same sorts of operations. (So we see that $\mathbb{R}^+$ is a subgroup of $\mathbb{C}^\times$.) Let ϕ be the function from $\mathbb{C}^\times$ to $\mathbb{R}^+$ defined by $\phi(a+bi)=a^2+b^2$, for all reals a and b that are not both 0. Prove that ϕ is a homomorphism from $\mathbb{C}^\times$ onto $\mathbb{R}^+$. Also discover what the kernel of ϕ is.

Solution
To see that ϕ is a homomorphism we need only establish

$$\phi\big((a+bi)(c+di)\big)=\phi(a+bi)\phi(c+di),$$

for all $a+bi, c+di\in\mathbb{C}^\times$. Here is the computation that demonstrates this.

$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i$$

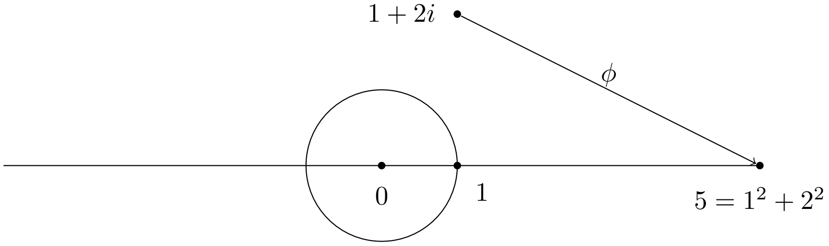
But then

$$\begin{aligned}\phi\big((a+bi)(c+di)\big) &= (ac-bd)^2+(bc+ad)^2\\ &= (ac)^2-2abcd+(bd)^2+(bc)^2+2abcd+(ad)^2\\ &= (ac)^2+(bd)^2+(bc)^2+(ad)^2\\ &= (ac)^2+(ad)^2+(bc)^2+(bd)^2\\ &= a^2(c^2+d^2)+b^2(c^2+d^2)\\ &= (a^2+b^2)(c^2+d^2)\\ &= \phi(a+bi)\phi(c+di)\end{aligned}$$

If $a \in \mathbb{R}^+$, then $\sqrt{a} = \sqrt{a}+0i \in \mathbb{C}^\times$ and $\phi(\sqrt{a}) = a$. This proves that ϕ maps $\mathbb{C}^\times$ onto $\mathbb{R}^+$.

Now the kernel of ϕ is the set of all complex numbers that ϕ maps to 1. That is $\ker\phi = \{a+bi \mid \phi(a+bi) = 1\}$. Since $\phi(a+bi) = a^2+b^2$, we see that $\ker\phi = \{a+bi \mid a^2+b^2 = 1\}$. This means that the kernel of ϕ is the set of complex numbers that lie on the unit circle centered at the origin.

There is a nice picture that goes with this.



Problem 45.

Let $\mathbf{G}$ be a group. Define $Z_G := \{g \mid g \in G \text{ and } gh = hg \text{ for all } h \in G\}$. Prove that $\mathbf{Z}_G$ is a normal subgroup of $\mathbf{G}$.

Solution

First we have to show that $Z_{\mathbf{G}}$ is a subgroup. All we need to do is check that it is closed under the operations of $\mathbf{G}$.

To see that $Z_{\mathbf{G}}$ is closed under the two-place operation, Let $g_0, g_1 \in Z_{\mathbf{G}}$ and pick an arbitrary $h \in G$. Then observe

$$(g_0g_1)h = g_0(g_1h) = g_0(hg_1) = (g_0h)g_1 = (hg_0)g_1 = h(g_0g_1).$$

In the line above we use $g_1h = hg_1$ and $g_0h = hg_0$. These two equations hold since $g_0, g_1 \in Z_{\mathbf{G}}$.

To see that $Z_{\mathbf{G}}$ is closed under formation of inverses, let $g \in Z_{\mathbf{G}}$. Let $h \in G$ be an arbitrary element of G. What we need is that $g^{-1}h = hg^{-1}$. Here is how to get it.

$$\begin{aligned} gh &= hg \text{ because } g \in Z_{\mathbf{G}}\\ h &= g^{-1}hg\\ hg^{-1} &= g^{-1}h\end{aligned}$$

Finally, we need $1 \in Z_{\mathbf{G}}$. This holds since for all $h \in G$ we know $h1 = h = 1h$.

So at this point we know that $Z_{\mathbf{G}}$ is a subgroup of $\mathbf{G}$.

To check that it is normal we need to show that $h^{-1}gh \in Z_{\mathbf{G}}$ whenever $h \in G$ and $g \in Z_{\mathbf{G}}$. But observe

$$h^{-1}gh = h^{-1}hg = 1g = g \in Z_{\mathbf{G}}.$$

Once again we use that $gh = hg$ since $g \in Z_{\mathbf{G}}$. So $Z_{\mathbf{G}}$ is a normal subgroup of $\mathbf{G}$.

This subgroup $\mathbf{Z_G}$ is called the **center** of $\mathbf{G}$. The "Z" comes from the German word "Zentrum" that corresponds to the American word "center" and the English word "centre".

Problem 46.
Let $\mathbf{G}$ be a group and let $\mathbf{H}$ and $\mathbf{K}$ be normal subgroups of $\mathbf{G}$ so that $H \cap K = \{1\}$. Prove that $hk = kh$ for all $h \in H$ and all $k \in K$.

Solution
Let $h \in H$ and $k \in K$. Notice that $hk = kh$ is logically equivalent to $h^{-1}k^{-1}hk = 1$. So we will prove the last equation.

Now $k^{-1} \in K$ since K is a subgroup (and so it is closed under inverses). Moreover, $h^{-1}k^{-1}h \in K$ because K is a normal subgroup and $h \in G$. Finally, $h^{-1}k^{-1}hk = \big(h^{-1}k^{-1}h\big)k \in K$ since it is the product of two things in K and K is closed under products.

In an entirely similar way, we see that $h^{-1}k^{-1}hk = h^{-1}\big(k^{-1}hk\big) \in H$.

So $h^{-1}k^{-1}hk \in H \cap K = \{1\}$. This means that $h^{-1}k^{-1}hk = 1$ as desired. Hence, $hk = kh$.

Problem Set 11
Due 12 November 2014

Problem 47.

Let $\mathbf{G}$ be the group of all 3×3 matrices with real entries that are invertible. The operations of this group are matrix multiplication, matrix inversion, and the identity matrix. Let S be the set of 3×3 matrices with real entries and with determinant 1. Let $\mathbb{R}^\times$ denote the group of nonzero numbers with the operations of multiplication, multiplicative inverse, and 1. Prove that $\mathbf{G}/S \cong \mathbb{R}^\times$. Does this hold when 3 is replaced by an arbitrary positive integer?

Solution

Let us define a map $d : G \to \mathbf{R}^\times$ by $d(M) = \det M$, the determinant of the matrix M. We know that a matrix is invertible if and only if its determinant is not zero. So the values d assigns to elements of G certainly belong to $\mathbb{R}^\times$. Another fact we know from linear algebra is that $d(MN) = d(M)d(N)$. Since we know that $\mathbf{G}$ and $\mathbb{R}^\times$ are groups, this means that d is a homomorphism. Does it map $\mathbf{G}$ onto $\mathbb{R}^\times$? Well, let r be any nonzero real number. Let M_r be the matrix with r as the upper left entry, with 1 at every other diagonal entry, and with 0 everywhere else. Then $d(M_r) = r$. In this way we see that d is a homomorphism from $\mathbf{G}$ onto $\mathbb{R}^\times$.

Now notice

$$\ker d = \{M \mid M \in G \text{ and } d(M) = 1\} = S.$$

So we conclude that S is a normal subgroup of $\mathbf{G}$ and that $\mathbf{G}/S \cong \mathbb{R}^\times$ by the Homomorphism Theorem.

That we were dealing with 3×3 matrices never came up in this line of reasoning, so the conclusion must be true when 3 is replaced by any $n > 0$.

Problem 48.

Let $\mathbf{G}$ be a finite group and n be a natural number. Prove that if $\mathbf{G}$ has exactly one subgroup of size n, then that subgroup must be normal.

Solution

Let H be the subgroup of order n. To see that H is a normal subgroup, let g be an arbitrary element of G. Our desire is to show that $H = g^{-1}Hg$.

We contend that $g^{-1}Hg$ is also a group of $\mathbf{G}$. Let us check this.

To pick a couple of elements of $g^{-1}Hg$ amounts to picking $h_0, h_1 \in H$, so our elements of $g^{-1}Hg$ are just $g^{-1}h_0g$ and $g^{-1}h_1g$. Observe

$$(g^{-1}h_0g)(g^{-1}h_1g) = g^{-1}h_0(gg{-}1)h_1g = g^{-1}(h_0h_1)g.$$

But we know $h_0h_1 \in H$ since H is closed under products. This entails that $g^{-1}Hg$ is closed under products.

Likewise $(g^{-1}hg)^{-1} = g^{-1}h^{-1}(g^{-1})^{-1} = g^{-1}h^{-1}g$. Here we see that for $h \in H$ we have also $h^{-1} \in H$, since H is closed under inversion. We conclude that $g^{-1}Hg$ is closed under inversion.

Finally, $1 = g^{-1}1g \in g^{-1}Hg$ since $1 \in H$.

Are H and $g^{-1}Hg$ the same size? consider the map $\Psi : H \to g^{-1}Hg$ defined by $\Psi(h) = g^{-1}hg$. This map is plainly onto. Is it one-to-one?

$$\begin{aligned}
\Psi(h_0) &= \Psi(h_1) \\
g^{-1}h_0g &= g^{-1}h_1g \\
gg^{-1}h_0g &= gg^{-1}h_1g \\
h_0g &= h_1g \\
h_0gg^{-1} &= h_1gg^{-1} \\
h_0 &= h_1
\end{aligned}$$

So yes, it is one-to-one.

But $\mathbf{G}$ has exactly one subgroup of size n and it is H. This means that $H = g^{-1}Hg$. Since this holds for arbitrary $g \in G$, we conclude that H is a normal subgroup of $\mathbf{G}$.

Problem 49.

Let X be an infinite set and σ be a permutation of X. We says that σ **moves only finitely many elements** provided the set $\{x \mid x \in X \text{ and } \sigma(x) \neq x\}$ is finite. Let

$$H = \{\sigma \mid \sigma \in \operatorname{Sym} X \text{ and } \sigma \text{ moves only finitely many elements}\}.$$

Prove that H is a normal subgroup of $\operatorname{Sym} X$.

Solution

In Problem 21 we already saw that H is a subgroup of $\operatorname{Sym} X$. To see that it is a normal subgroup, let $\sigma \in H$ and $\tau \in \operatorname{Sym} X$. All be need to do is show that $\tau^{-1} \circ \sigma \circ \tau$ moves only finitely many points. Let F be the subset of X consisting of all points moved by σ. We know that F is finite. Let Y consist of those points in X that are mapped to points in F. Notice that Y is the same size as X since τ is one-to-one and it maps Y onto F. Now let $x \in X$ so that $x \notin Y$. Then $\tau(x) \notin F$. So $\sigma(\tau(x)) = \tau(x)$. But this means $\tau^{-1}(\sigma(\tau(x))) = \tau^{-1}(\tau(x)) = x$. So $\tau^{-1} \circ \sigma \circ \tau$ fixes every point not in Y. Since Y is finite, $\tau^{-1} \circ \sigma \circ \tau$ can move only finitely many points. This means that $\tau^{-1} \circ \sigma \circ \tau \in H$. Therefore H is a normal subgroup of $\operatorname{Sym} X$.

Problem 50.

Let $\mathbf{G}$ be a group, let $\mathbf{H}$ be a subgroup of $\mathbf{G}$, and let $\mathbf{N}$ be a normal subgroup of $\mathbf{G}$. Prove each of the following.

(a) NH is a subgroup of $\mathbf{G}$.

(b) N is a normal subgroup of NH.

(c) $N \cap H$ is a normal subgroup of $\mathbf{H}$.

(d) $\mathbf{H}/(N \cap H) \cong NH/N$.

Solution

Let us first do part (a). To check that NH is closed under products, pick $n_0, n_1 \in N$ and $h_0, h_1 \in H$. So n_0h_0 and n_1h_1 are arbitrary elements of NH. Observe

$$(n_0h_0)(n_1h_1) = n_0h_0n_1(h_0^{-1}h_0)h_1 = n_0(h_0n_1h_0^{-1})(h_0h_1).$$

But $h_0n_1h_0^{-1} \in N$ since N is normal. Thus $n_0(h_0n_1h_0^{-1}) \in N$ since N is closed under products. Likewise $h_0h_1 \in H$ since H is closed under products. In this way we see that $(n_0h_0)(n_1h_1)$ is the product of an element of N with an element of H. So NH is closed under products.

The set NH is also closed under inversion. Here is why. Let $n \in N$ and $h \in H$. So nh is an arbitrary element of NH. Now $(nh)^{-1} = h^{-1}n^{-1} = h^{-1}n^{-1}hh^{-1} = (h^{-1}n^{-1}h)h^{-1}$. But $n^{-1} \in N$ since N is closed under inversion. Moreover, $h^{-1}n^{-1}h \in N$, since N is normal. But also $h^{-1} \in H$ since H is closed under inversion. Altogether, we see that $(nh)^{-1}$ is a product of an element of N with an element of H. So NH is closed under inversion.

Of course, $1 = 1 \cdot 1 \in NH$.

So NH is a subgroup of $\mathbf{G}$.

Part (b) is too easy (but students should write out the details for practice).

Now we do parts (c) and (d) simultaneously by appealing to the Homomorphism Theorem. Let $\phi : H \to NH/N$ be defined by $\phi(h) = hN$. We need to prove three things: that ϕ is a homomorphism, that ϕ maps H onto NH/N, and that $\ker \phi = N \cap H$. Then a direct appeal to the Homomorphism Theorem does the trick.

To check that ϕ is a homomorphism, it suffices to show that it preserves the product since we already know that $\mathbf{H}$ and NH/N are groups. So let $h_0, h_1 \in H$. We see that $\phi(h_0h_1) = (h_0h_1)N = (h_0N)(h_1N)$ since this is the way that products work in quotient groups. But this gives $\phi(h_0h_1) = \phi(h_0)\phi(h_1)$, as desired.

Is ϕ onto? Well, pick $n \in N$ and $h \in H$. So the coset $(nh)N$ is an arbitrary element of NH/N. By normality $h^{-1}n^{-1}h \in N$. This means $nh(h^{-1}n^{-1}h) \in (nh)N$. But $nhh^{-1}n^{-1}h = h$. So we find that $h \in (nh)N$. Since

$h \in hN$ as well we see that the cosets $(nh)N$ and hN have an element in common. So they must be the same. That is $(nh)N = hN = \phi(h)$. In this way we see that every element of NH/N is the image under ϕ of some element of H.

The last thing we need to do is understand the kernel of ϕ.

$$\begin{aligned} h \in \ker\phi &\text{ if and only if } \phi(h) = 1N = N \text{ and } h \in H \\ &\text{ if and only if } hN = N \text{ and } h \in H \\ &\text{ if and only if } h \in N \text{ and } h \in H \\ &\text{ if and only if } h \in N \cap H \end{aligned}$$

So the sets $\ker\phi$ and $N \cap H$ have the same elements. This means $\ker\phi = N \cap H$.

Problem Set 12
Due 19 November 2014

Problem 51.
Let $\mathbf{G}$ be a group and let $\mathbf{H}$ and $\mathbf{K}$ be subgroups of $\mathbf{G}$. Prove $|HK||H \cap K| = |H||K|$. [Hint: Lagrange's Theorem or its proof helps. Warning: we do not assume that either of the subgroups is normal.]

Solution
The set HK is the disjoint union of left cosets of the form hK where $h \in H$. We know from Lagrange that $|hK| = |K|$. So to figure out $|HK|$ we only need to see how many of these left cosets there are. We have to be careful about counting things more than once. Well, suppose $h_0, h_1 \in H$ and $h_0K = h_1K$. But this means $h_1^{-1}h_0 \in K$. From this we get $h_1^{-1}h_0 \in H \cap K$. But this is the same as $h_0(H \cap K) = h_1(H \cap K)$. In this way we see that HK is partitioned in the same number of left cosets of K as H is partitioned into left cosets of $H \cap K$. This last is just the index $[H : H \cap K]$ of $H \cap K$ in H. So we find $|HK| = [H : H \cap K]|K|$. This leads to $|HK||H \cap K| = [H : H \cap K]|H \cap K||K|$. But Lagrange told us $|H| = [H : H \cap K]|H \cap K|$. So we arrive at $HK||H \cap K| = |H||K|$ as desired.

Problem 52.
Let $\mathbf{G}$ be a group and let $\mathbf{H}$ be a subgroup of $\mathbf{G}$ so that $[\mathbf{G} : \mathbf{H}] = 2$. Prove that $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

Solution
By Lagrange, we know that G is partitioned into left cosets of H. Our hypothesis is that there are exactly two such cosets. One, of course, must be H itself. The other must be $G \setminus H$, since there are only two pieces. That is $G \setminus H$ is a left coset of H. Now we can reason exactly the same way to conclude that $G \setminus H$ is also a right coset of H. Now one of the characterization of normality is that a subgroup $\mathbf{H}$ is normal if and only if every left coset of H is also a right coset of H. But let us see this more directly. Suppose $h \in H$ and $g \in G$. We must deduce that $g^{-1}hg \in H$. Now $Hg = gH$. Since $hg \in Hg = gH$, we can pick $h' \in H$ so that $hg = gh'$. But then $g^{-1}hg = g^{-1}gh' = h' \in H$, as desired.

Problem 53.
Suppose that $\mathbf{N}$ is a normal subgroup of the group $\mathbf{G}$ and the $\mathbf{N}$ is a *finite* cyclic group. Prove that every subgroup of $\mathbf{N}$ is a normal subgroup of $\mathbf{G}$.

Solution
Let $\mathbf{H}$ be a subgroup of $\mathbf{N}$ and $g \in G$. We must see that $g^{-1}Hg = H$. First, observe that $g^{-1}Hg \subseteq N$ since $\mathbf{N}$ is a normal subgroup of $\mathbf{G}$. Now $\mathbf{N}$ is a finite cyclic group and such groups can have at most one subgroup of any given cardinality. So $\mathbf{H}$ is the only subgroup of $\mathbf{N}$ of its size. So we can finish this problem by proving two things: that $g^{-1}Hg$ is a subgroup of $\mathbf{N}$ and that it is the same size as H.

$g^{-1}Hg$ contains 1
Well, $1 \in H$ since $\mathbf{H}$ is a subgroup. But then $1 = g^{-1} \cdot 1 \cdot g \in g^{-1}Hg$.

$g^{-1}Hg$ is closed under the formation of inverses
Let $h \in H$. Observe $(g^{-1}hg)^{-1} = g^{-1}h^{-1}(g^{-1})^{-1} = g^{-1}h^{-1}g \in g^{-1}HG$, because $h^{-1} \in H$, since $\mathbf{H}$ is a subgroup.

$g^{-1}Hg$ is closed under the formation of products
Let $h_0, h_1 \in H$. Then observe $g^{-1}h_0gg^{-1}h_1g = g^{-1}h_0h_1g \in g^{-1}Hg$, because $h_0h_1 \in H$, since$\mathbf{H}$ is a subgroup.

So $g^{-1}Hg$ is a subgroup of $\mathbf{N}$.

To see that $|H{=}g^{-1}Hg|$, consider the map $\Phi : H \to g^{-1}Hg$ defined by $\Phi(h) := g^{-1}hg$ for all $h \in H$. We need to show that Φ is one-to-one and that it maps H onto $g^{-1}Hg$. The onto part is evident from the definitions. To see the one-to-oneness suppose that $\Phi(h_0) = \Phi(h_1)$. This means that $g^{-1}h_0g = g^{-1}h_1g$. But then $h_0 = gg^{-1}h_0gg^{-1} = gg^{-1}h_1gg^{-1} = h_1$, as desired.

Problem 54.
Let $\mathbf{G}$ be a group with exactly 2 subgroups. Prove that $\mathbf{G} \cong \mathbb{Z}_p$ for some prime number p.

Solution
Well, we know that the trivial subgroup and the whole group are always subgroups. It is possible that these subgroups are the same. In that case, our group must be the trivial group: the group with one element. The trivial group has only one subgroup. So the group given in this problem cannot be t he trivial group. This means it has some element other than the identity element. Let a be such an element. Now the set $\{a^k \mid k \in \mathbb{Z}\}$ is easily seen to be closed under all the group operations. So it is a nontrivial subgroup, in fact it is the subgroup generated by a. Since $\mathbf{G}$ has exactly two subgroups, we see that $G = \{a^k \mid k \in \mathbb{Z}\}$. So we see that $\mathbf{G}$ is a cyclic group, and more that it is generated by any of its elements that are different from 1. At this point we certainly know that $\mathbf{G}$ must be isomorphic to $\mathbb{Z}$ or to some $\mathbb{Z}_n$ where n is a natural number with $1 < n$. But $\mathbb{Z}$ has infinitely many subgroups, for example the subgroup consisting of all multiples of 17. So it can't be $\mathbb{Z}$. Also, we know that if $m|midn$, then $\mathbb{Z}_n$ as a (exactly one) subgroup of order m. So if $\mathbb{Z}_n$ is to have exactly two subgroups, it must be that n has exactly two divisors among the natural numbers. This means that n must be prime.

Problem Set 13
Due 24 November 2014

Problem 55.
Let $\mathbf{G}$ be a finite group and let $\mathbf{H}$ and $\mathbf{K}$ be subgroups of $\mathbf{G}$. Suppose that $|H|$ and $|K|$ are relatively prime. Prove that $H \cap K = \{1\}$.

Solution
We know that $H \cap K$ is a subgroup of both $\mathbf{H}$ and $\mathbf{K}$. So Lagrange tells us that $|H \cap K|$ must divide both $|H|$ and $|K|$. But these number are relatively prime. So $|H \cap K| = 1$. Since the identity element belongs to every subgroup, it must be the only element of $H \cap K$. So $H \cap K = \{1\}$.

Problem 56.
Let $\mathbf{G}$ be a group and let $a \in G$. Define $F_a : G \to G$ via $F_a(x) = axa^{-1}$ for all $x \in G$. Prove that F_a is an isomorphism from $\mathbf{G}$ onto $\mathbf{G}$.

Solution
To see that F_a is one-to-one and that it maps G onto G we show it has a two-sided inverse. Define $H_a : G \to G$ by $H_a(x) = a^{-1}xa$ for all $x \in G$. Then just observe

$$H_a(F_a(x)) = H_a(axa^{-1}) = a^{-1}axa^{-1}a = x$$

and

$$F_a(H_a(x)) = F_a(a^{-1}xa) = a^{-1}axa^{-1}a = x.$$

So F_a is one-to-one and maps G onto G. Since $\mathbf{G}$ is a group, to see that F_a is also a homomorphism, we only have to show it preserves the group product. Here is how:

$$F_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1}) = F_a(x)F_a(y).$$

Problem 57.
Let $\mathbf{A}, \mathbf{B}$, and $\mathbf{C}$ be rings. Let h be a homomorphism from $\mathbf{A}$ onto $\mathbf{B}$ and let g be a homomorphism from $\mathbf{A}$ onto $\mathbf{C}$ such that $\ker h = \ker g$. Prove that there is an isomorphism f from $\mathbf{B}$ onto $\mathbf{C}$.

Solution
Here are two ways to do this problem.

The first way invokes the Homomorphism Theorem twice: by that theorem we see that

$$\mathbf{B} \cong \mathbf{A}/\ker h \text{ and } \mathbf{C} \cong \mathbf{A}/\ker g.$$

Since $\ker h = \ker g$ we can rewrite this as

$$\mathbf{B} \cong \mathbf{A}/\ker h = \mathbf{A}/\ker g \cong \mathbf{C},$$

provided we know that $\cong$ is a symmetric relation—that is that the inverse of an isomorphism is an isomorphism (about this see Problem 14). Then, provided we know that $\cong$ is transitive (see Problem 15), we draw the desired conclusion that $\mathbf{B} \cong \mathbf{C}$.

The second way defines the desired isomorphism f directly by

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

So we see that f is a subset of $B \times C$. We need to establish five things about f:

- f is a function.
- f is one-to-one.

- The domain of f is B.
- f maps B onto C.
- f is a homomorphism.

To see that f is a function, we invoke the "vertical line test". So suppose $(b,c),(b,c') \in f$. We have to show that $c = c'$. From the first pair and the definition of f select $a \in A$ so that $h(a) = b$ and $g(a) = c$. From the second pair and the definition of f select $a' \in A$ so that $h(a') = b$ and $g(a') = c'$. Because $h(a) = b = h(a')$, we find that $(h(a))^{-1}h(a') = 1$. But h is a homomorphism, so $h(a^{-1}a') = 1$. This means that $a^{-1}a' \in \ker h$. Since the $\ker h = \ker g$. We have that $a^{-1}a' \in \ker g$. Hence $(g(a))^{-1}g(a') = 1$. But this gives $g(a) = g(a')$, or what is the same $c = c'$. Here we only used that $\ker h \subseteq \ker g$.

At this point, we see that $f(h(a)) = g(a)$ is another way to write $((h(a),g(a)) \in f$.

To see that f is one-to-one, we invoke the "horizontal line test". So suppose $(b,c),(b',c) \in f$. We have to show that $b = b'$. Compared to the paragraph above all we are doing is interchanging the roles of B and C. So you should complete this argument by following the pattern above. This time use that $\ker g \subseteq \ker h$.

To see that the domain of f is the whole set B, let $b \in B$. Because h maps A onto B, we can pick $a \in A$ so that $h(a) = b$. But then $(h(a),g(a)) \in f$ and $b = h(a)$ is in the domain of f.

To see that f maps B onto C, let $c \in C$. Because g maps A onto C, we can pick $a \in A$ so that $g(a) = c$. Thus $(h(a),g(a)) = (h(a),c) \in f$. So f maps B onto C.

To see that f is a homomorphism, we only need to see that the group product is preserved, since we know that $\mathbf{B}$ and $\mathbf{C}$ are groups. So let $b,b' \in B$. Using the ontoness of h pick $a,a' \in A$ so that $h(a) = b$ and $h(a') = b'$. So we have

$$f(bb') = f(h(a)h(a')) = f(h(aa')) = g(aa') = g(a)g(a') = f(h(a))f(h(a')) = f(b)f(b').$$

In this chain of equalities we used that h and g preserve products.

This second proof resembles the proof of the Homomorphism Theorem.

Problem 58.

Let $\mathbf{G}$ be a group and let H, K, and N be subgroups of $\mathbf{G}$ fulfilling all the following conditions:

- $H \subseteq K$,
- $HN = KN$,
- $H \cap N = K \cap N$.

Under these stipulations, prove that $H = K$.

Solution

Since we are given $H \subseteq K$ it only remains to see that $K \subseteq H$. So let $k \in K$. Then $k = k \cdot 1 \in KN = HN$. So pick $h \in H$ and $n \in N$ so that $k = hn$. This yields $h^{-1}k = n$. Now $h^{-1} \in H$ since H is a subgroup. Also $h^{-1} \in K$ since $H \subseteq K$. But K is a subgroup, so $h^{-1}k \in K$. This means that $n \in K$. But we know $n \in N$. So $n \in K \cap N = H \cap N$. We deduce that $h^{-1}k = n \in H$. So $k = hn \in H$ since H is a subgroup. We just saw that $k \in H$. But k was an arbitrary element of K, so we conclude that $K \subseteq H$, as desired.