

SOLUTIONS FOR THE TRAINING FINAL

Remember : the final exam is cumulative, though there will be more questions on the last third of the program. This is a set of training exercises on that last third (Groups action, rings and fields).

1.- Let R be a ring with unity, R^* the groups of unit.

a.- Show that the application $R^* \times R \rightarrow R$, $(g, x) \mapsto gx$ is an action of the group R^* on the set R .

b.- Let x in R , and let G_x be its stabilizer for the action of R^* . Show that if x is not a divisor of 0, then $G_x = \{1\}$.

c.- Take $R = \mathbb{Z}_{10}$. Write down the orbits of the action described above.

Solution: a.- We use the notation \bullet for this action, so that $g \bullet x = gx$. We have to check that for g, g' in \mathbb{R}^* and $x \in \mathbb{R}$, $g \bullet (g' \bullet x) = (gg') \bullet x$, which amounts to $g(g'x) = (gg')x$, and this is true by associativity of the multiplication of \mathbb{R} . We also have to check that $1 \bullet x = x$, and this amounts to $1x = x$ which is clear.

b.- G_x is the set of g 's such that $g \bullet x = x$, that is $gx = x$ or $(g - 1)x = 0$. If $x \neq 0$, this implies $g - 1 = 0$ that is $g = 1$.

c.- the element of $(\mathbb{Z}_{10})^*$ are the classes of integer prime to 10, that is 1, 3, 7, 9. The orbits are $\{0\}$, $\{1, 3, 7, 9\}$, $\{2, 6, 4, 8\}$, $\{5\}$.

2.- Let R be a ring of characteristic 2.

a.- Show that for all $x \in R$, we have $x = -x$.

b.- Show that if R is commutative, then for all $x, y \in R$, $(x + y)^2 = x^2 + y^2$.

c.- Conversely, show that if for all $x, y \in R$, $(x + y)^2 = x^2 + y^2$, then R is commutative.

Solution a.- By definition, we have for all $x \in \mathbb{R}$ $2x = 0$. That is $x + x = 0$, and by adding $-x$, $x = -x$.

b.- In any ring, we have by distributivity $(a + b)^2 = a^2 + ab + ba + a^2$. If the ring is commutative, then $ab = ba$, and we have $(a + b)^2 = a^2 + 2ab + b^2$. If the ring has characteristic 2 moreover $2xy = 0$ and $(x + y)^2 = x^2 + y^2$.

c.- By the computations in b.- above, for all $x, y \in R$, the relation $(x + y)^2 = x^2 + y^2$ implies $xy + yx = 0$ or $xy = -yx$. By a.- $-yx = yx$, so $xy = yx$.

3.- Let R be the ring $\mathbb{Z} \times \mathbb{Z}$.

a.- Show that R has a unity.

b.- What are the divisors of 0 in R .

c.- What are the units of R . Is the group R^* cyclic ?

Solutions: a.– $(1, 1)$ is obviously the unity of \mathbb{R} .

b.– (x, y) is a divisor of 0 if there exists (x', y') not equal to $(0, 0)$ such that $(xx', yy') = (0, 0)$. If both x and y are different from 0, this implies $x' = 0$ and $y' = 0$ so (x, y) is not a divisor of 0. If x is 0 however, then one can take $(x', y') = (0, 1)$ for instance, and we see that $(0, y)$ is a divisor of 0. Similarly if $y = 0$. So the divisor of 0 is the set of (x, y) such that x or y is 0.

c.– The units are the (x, y) with either x or y is equal to 1 or -1 . The groups of units have therefore four elements, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. It is not cyclic.

4.– Solve the congruence

$$7x \equiv 11 \pmod{20}$$

Solutions: In \mathbb{Z}_{20} , the inverse of $\bar{7}$ is $\bar{3}$. So the solution of $\bar{7}x = \bar{11}$ in \mathbb{Z}_{20} is $\bar{3} \times \bar{11} = \bar{13}$. The solution of the congruence is therefore the set of all integers congruent to 13 modulo 20 : $\dots, -27, -7, 13, 33, 53, \dots$

5.– Solve the equation $\bar{12}x = \bar{23}$ in \mathbb{Z}_{50} .

Solutions: The g.c.d of 12 and 50 is 4, and 4 does not divides 23. Therefore, the congruence has no solutions.

6.– Solve the equation $\bar{4}x = \bar{6}$ in \mathbb{Z}_{10} .

Solution: The gcd of 4 and 10 is 2, and 2 divides 6. Therefore the equations has 2 solutions. To find them, we divides everything by 2, solving $\bar{2}x = \bar{3}$ in \mathbb{Z}_5 , a solution that has one solution $\bar{4}$ in \mathbb{Z}_5 . The solution of the original equations are the integers modulo 10 that are congruent to $\bar{4}$ modulo 5, that is $\bar{4}$ and $\bar{9}$.

7.– Compute $\phi(18)$. Compute $5^{1000} \pmod{18}$.

Solutions: $\phi(18)$ is the number of integer prime to 18 between 1 and 18. Those are 1, 5, 7, 11, 13, 17, so $\phi(18) = 6$. By Euler's theorem, since 5 is relatively prime to 18, we have $5^6 \equiv 1 \pmod{18}$. We compute

$$5^{1000} \equiv 5^{6 \times 166 + 4} \equiv (5^6)^{166} \times 5^4 \equiv 5^4 \equiv 13 \pmod{18}.$$

8.– Let p be a prime number different from 2 and 5. Show that p divides an integer with only 9 in its decimal writing (that is 9999...999.) You may use Fermat's little theorem.

Solutions: Since 10 is relatively prime to p , we have $10^{p-1} \equiv 1 \pmod{p}$, so p divides $10^{p-1} - 1$ which is the number with exactly $p - 1$ times the digit 9 in its decimal writing.

9.– Let C be the ring of all continuous function from \mathbb{R} to \mathbb{R} . Is C a domain?

Solution: No. indeed, consider the function $f(x)$ whose value is 0 if $x \leq 0$ and x if $x \geq 0$. This function is continuous on \mathbb{R} , so that is an element of C .

Similarly, consider the function $g(x)$ whose value is 0 if $x \geq 0$ and x if $x \leq 0$. This is also continuous. Now $f(x)g(x) = 0$ for all x , which means that the product of f and g is 0 in C , while neither f nor g is 0.

10.– Let R be the set of all rational numbers that can be written $\frac{a}{2^n}$ where a is an integer and n a non negative integer.

a.– Show that R is a subring of \mathbb{Q} . Show that it is a domain. Is it a field?

Solution. R is a subset of \mathbb{Q} . To show that it is a subring, we have to check that it is closed by addition (clear since $a/2^n + b/2^m = (a2^m + b2^n)/2^{n+m}$, that it contains the neutral element for the addition ($0 = 0/2^0$), the additive inverse of any element $-(a/2^n) = (-a/2^n)$, and that it is closed by multiplication (clear). It contains also the unity $1 = 1/2^0$, and it is commutative as a subring of \mathbb{Q} which is so. It is a domain since \mathbb{Q} is. But it is not a field, since 3, for instance, has no inverse.

b.– What are the units of R ? To which group is R^* isomorphic?

Answer: (more justification is needed to get full credit) The units are the elements of the form $\pm 2^n$, for $n \in \mathbb{Z}$. The group of units R^* is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

c.– What is the field of fraction of R ?

Solution: Let us call F the field of fraction R . Since \mathbb{Q} is a field that contains R , we have $F \subset \mathbb{Q}$ (by the theorem 2 on field of fractions). But F contains R so it contains \mathbb{Z} , so F contains the field of fraction \mathbb{Q} of \mathbb{Z} . So $\mathbb{Q} \subset F$, and actually $F = \mathbb{Q}$.