MAT 512 Exam 2 Solutions

Solutions are due at the beginning of class on **Monday, April 17**.

1. Let R be a ring. As usual, we denote by $-a \in R$ the additive inverse of an element $a \in R$. Give a careful proof, referring to the conditions in the definition of a ring where necessary, for the following fact: for every element $a \in R$, one has $(-1) \cdot a = -a$.

Solution: Let us first prove that $0 \cdot a = 0$ for $a \in R$. Temporarily set $b = 0 \cdot a$. Then

$$b + b = 0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a = b,$$

due to the distributive law and the fact that 0 is the additive identity. We can now add $-b$ on both sides and use the associative law to get

$$0 = b + (-b) = (b + b) + (-b) = b + \big(b + (-b)\big) = b + 0 = b,$$

which gives the desired conclusion $0 \cdot a = b = 0$.

Now let us prove that $(-1) \cdot a = -a$. For that, we need to show that $(-1) \cdot a$ is the additive inverse of a. This is true because of the following calculation:

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = \big(1 + (-1)\big) \cdot a = 0 \cdot a = 0.$$

Here we used the fact that 1 is the multiplicative identity; the distributive law; the fact that -1 is the additive inverse of 1; and the fact that $0 \cdot a = 0$.

2. Let K be a field, and consider the polynomial $x - r \in K[x]$, where $r \in K$ is an arbitrary element. Show that if $x - r$ divides the product $f(x)g(x)$ of two polynomials $f(x), g(x) \in K[x]$, then $x - r$ must divide one of the two factors of the product. (You are not allowed to use Bézout's theorem!)

Solution: We showed in class that a polynomial $f(x) \in K[x]$ is divisible by $x - r$ if and only if $f(r) = 0$. Since $x - r$ divides $f(x)g(x)$, this means that $f(r)g(r) = 0$. Because K is a field (and therefore without zero divisors), it follows that $f(r) = 0$ or $g(r) = 0$. In the first case, $x - r$ divides $f(x)$; in the second case, $x - r$ divides $g(x)$.

3. Let p be a prime number. Determine how many irreducible polynomials of the form $x^2 + ax + b$ there are in the ring $\mathbb{Z}_p[x]$. Explain clearly how you arrived at your answer. (How many polynomials of the form $x^2 + ax + b$ are there in total? How many of these can be written as a product $(x + c)(x + d)$ of two linear polynomials?)

Solution: A (monic) quadratic polynomial is either irreducible, or the product of two (monic) linear polynomials. All we have to do is find how many quadratic polynomials there are, and then subtract the number of those that can be written as a product of two linear polynomials. There are clearly p^2 many polynomials of the form $x^2 + ax + b$ in the

ring $\mathbb{Z}_p[x]$, because there are exactly p possibilities for each of the two coefficients. The number of polynomials that factor as $(x+c)(x+d)$ is

$$\frac{p(p-1)}{2} + p = \frac{p(p+1)}{2}.$$

Indeed, when $c \neq d$, there are $p(p-1)$ ways of choosing c and d, but we have to divide this number by 2 because $(x+c)(x+d)$ and $(x+d)(x+c)$ are of course the same polynomial. There are also exactly p polynomials of the form $(x+c)^2$. It follows that the number of irreducible monic polynomials in $\mathbb{Z}_p[x]$ is

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}.$$

4. Let p be a prime number. Explain clearly why every element of $\mathbb{Z}_p$ is a root of the polynomial $x^p - x \in \mathbb{Z}_p[x]$. Use this to write $x^p - x$ as a product of linear polynomials.

Solution: We can use Fermat's theorem, which says that $a^{p-1} = 1$ for every nonzero element $a \in \mathbb{Z}_p$. It follows that $a^p = a \cdot a^{p-1} = a$, and so a is a root of the polynomial $x^p - x$. The only remaining element is $0 \in \mathbb{Z}_p$, which is clearly also a root. Therefore every element of $\mathbb{Z}_p$ is a root of the polynomial $x^p - x$. Since every root leads to a linear factor, this gives us the following factorization:

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a).$$

5. Suppose that R is a ring in which

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ terms}} = 0$$

for some $m \geq 1$. The smallest number m with this property is called the *characteristic* of the ring R. Show that if R is an integral domain, then the characteristic must be a prime number. Be sure to explain your reasoning clearly.

Solution: Let $m \geq 1$ be the characteristic of the integral domain R. Since $1 \neq 0$ in an integral domain, we cannot have $m = 1$, and so $m \geq 2$. Now we use a proof by contradiction. Suppose that m is not a prime number. This means that it has a nontrivial factorization $m = k\ell$ into two smaller integers k, ℓ. Using the distributive law several times, we get

$$\underbrace{(1 + 1 + \cdots + 1)}_{k \text{ terms}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{\ell \text{ terms}} = \underbrace{1 + 1 + \cdots + 1}_{k\ell \text{ terms}} = 0.$$

Since R is an integral domain, one of the two factors must be equal to 0. But because $k < m$ and $\ell < m$, this contradicts the fact that m was supposed to be the smallest integer with this property. Therefore m must be a prime number.