

MAT 444: Test 2 Solutions

1. Define the following terms

(a) *Sylow subgroup*

If G is a finite group, p a prime and $|G| = p^n m$ where $p \nmid m$, a *Sylow p -subgroup* is a subgroup of order p^n .

(b) *Unit in a ring*

If R is a ring with one, an element $a \in R$ is a unit if there exists b in R such that $ab = ba = 1_R$.

(c) *Prime ideal*

If R is a commutative ring and I is an ideal of R , then I is a *prime ideal* if I is a proper ideal and if for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

2. Determine all irreducible polynomials of degree 3 in $\mathbb{Z}_2[x]$ and prove your answer.

Let $f = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}_2[x]$. Since $\mathbb{Z}_2 = \{0, 1\}$ and $a_3 \neq 0$, $a_3 = 1$. Since $\mathbb{Z}_2$ is a field, and polynomial of degree 3 is irreducible if and only if it has no roots. So, f is irreducible iff

$$a_0 = f(0) \neq 0 \text{ and } 1 + a_2 + a_1 + a_0 = f(1) \neq 0.$$

So, $a_0 = 1$ (the only non-zero value) and f is irreducible iff

$$1 + a_2 + a_1 + 1 = 1 \iff a_1 + a_2 = 1.$$

But the only combinations which work are $(a_1 = 1 \text{ and } a_2 = 0)$ or $(a_1 = 0 \text{ and } a_2 = 1)$. Thus, the irreducible polynomials of degree 3 in $\mathbb{Z}_2[x]$ are

$$x^3 + x^2 + 1 \text{ and } x^3 + x + 1.$$

3. Let R be a commutative ring with $1 \neq 0$ and $a \in R$. Let $f_a: R \rightarrow R$ be given by $f_a(r) = ar$.

(a) Prove that if f_a is one-to-one, then $a \neq 0$ and a is not a zero-divisor.

If $a = 0_R$, then $f_a(0_R) = 0_R \cdot 0_R = 0_R = 0_R \cdot 1_R = f_a(1_R)$, so f is not one-to-one (since $0_R \neq 1_R$).

Now suppose a is a zero-divisor. Then there exists $b \neq 0$ such that $ab = 0_R$ and

$$f_a(b) = ab = 0_R = a \cdot 0_R = f_a(0_R)$$

Since $b \neq 0_R$, this contradicts that f_a is one-to-one.

(b) Prove that $I = \{r \in R \mid f_a(r) = 0_R\}$ is an ideal of R .

Note, we do not have that f_a is a homomorphism, so we cannot just apply a standard property of the kernel. First, $f_a(0) = a \cdot 0 = 0$, so $0 \in I$. Next, if $b, c \in I$, then $f_a(b) = 0$ and $f_a(c) = 0$, which implies $ab = 0$ and $ac = 0$. But then $f_a(b - c) = a(b - c) = ab - ac = 0 - 0 = 0$. Thus, $b - c \in I$. Finally, suppose $b \in I$ and $r \in R$. Then $f_a(b) = 0$, so $f_a(br) = a(br) = (ab)r = 0 \cdot r = 0$. Thus $br \in I$. Since R is a commutative ring, $br = rb$ and we get $rb \in I$ too.

- (c) *Prove that if $a^2 = a$, then f_a is a ring homomorphism.*

If $b, c \in R$, then

$$f_a(bc) = a(bc) = a^2(bc) = (ab)(ac) = f_a(b)f_a(c)$$

and

$$f_a(b+c) = a(b+c) = (a+b)(a+c) = f_a(b) + f_a(c)$$

So, f_a is a homomorphism.

4. Suppose G acts on a set A and $a \in A$.

- (a) *Define, $\mathcal{O}_a$, the orbit of a .*

The orbit of a is

$$\mathcal{O}_a = \{g \cdot a \mid g \in G\}$$

- (b) *Define, G_a , the isotropy subgroup of a .*

The isotropy subgroup of a is

$$G_a = \{g \in G \mid g \cdot a = a\}$$

- (c) *Prove $|\mathcal{O}_a| = [G : G_a]$.*

Let L be the set of left cosets of G_a , so. Define the function

$$\begin{aligned} f : L &\rightarrow G_a \\ gG_a &\mapsto g \cdot a \end{aligned}$$

We check that f is well-defined.

Suppose $g_1G_a = g_2G_a$. Then $g_1 = g_2h$ for some $h \in G_a$ and

$$g_1a = (g_2h)a = g_2(ha) = g_2a$$

where the last equality follows from the fact that $h \in G_a$. So, f is well-defined.

For any $ga \in \mathcal{O}_a$, $ga = f(gG_a)$, so f is onto. Finally, we show f is 1-1. Suppose $f(g_1G_a) = f(g_2G_a)$. Then

$$\begin{aligned} g_1a = g_2a &\implies g_1^{-1}g_1a = g_1^{-1}g_2a \\ &\implies 1 \cdot a = (g_1^{-1}g_2)a \\ &\implies a = (g_1^{-1}g_2)a \end{aligned}$$

So, $g_1^{-1}g_2 \in G_a$, which implies $g_1G_a = g_2G_a$. Thus f is injective, and we already showed it was surjective, so it is bijective proving $[G : G_a] = |L| = |\mathcal{O}_a|$.

5. Let G be a group of order $1225 = 5^2 \cdot 7^2$.

- (a) *Prove that G is not a simple group.*

Let n_p be the number of Sylow p -subgroups. From the 3rd Sylow theorem, $n_5 \mid 7^2$, so $n_5 = 1, 7$ or 49 . Also, $n_5 \equiv 1 \pmod{5}$, and the only value satisfying this is $n_5 = 1$ (the others are congruent to 2 and 4). So, there is a unique Sylow 5-subgroup H , which is then normal (since it is the only subgroup of order 25). Since it has order 25, it is non-trivial and proper. Thus G is not simple.

(b) *Prove that G is abelian.*

From the 3rd Sylow theorem, we also have that $n_7 \mid 5^2$, so $n_7 = 1, 5$, or 25 . The only one of these congruent to 1 modulo 7 is 1. So, the Sylow 7 subgroup, K , is also normal (unique subgroup of that order).

By a theorem of the course, if a group has order equal to the square of a prime, then the group is abelian. Thus, both H and K are abelian.

Since H and K are both normal subgroups, HK is a subgroup of G . The order of $H \cap K$ divides both $|H| = 5^2$ and $|K| = 7^2$, so $|H \cap K| = 1$. By the direct product recognition theorem, $HK \cong H \times K$.

Moreover, $|HK| = |H \times K| = |H| \cdot |K| = 5^2 \cdot 7^2 = |G|$, so $G = HK$. Thus, $G \cong H \times K$, the product of two abelian groups, and so G is abelian.

Note, one could go further and use that we know the two groups of order p^2 to produce the four combinations for G , which would completely classify the groups of order 1225 up to isomorphism.