MAT2200: Mandatory assignment

Jon-Magnus Rosenblad

Problem 1

1.

Let G be a group of even order. Since every element of G must have it's own unique inverse, and since the inverse property is symmetric, every element can be paired with it's inverse (possibly itself) so that element will appear in exactly one pair. Since the identity e is it's own inverse it cannot be paired to any other element. Now we have an odd number of elements to pair, so at least one element, int addition to e, must be it's own inverse.

Let $g \in G$ be an element s.t. $g \neq e$ and $g = g^{-1}$. Clearly $\langle g \rangle$ is a subgroup of G of order 2. Let $H = G/\langle g \rangle$ be a quotient group of G. Assume there exists some $a \in G$ of order 2 different from g. Then $\exists h \in H \quad a \in h$ and $a^2 = e \in h^2$ so $h^2 = e_H$. Then the other element i h, namely ga has the property that $(ga)^2 = gaga \in e_H$, so $gaga = g$ or $gaga = e$.

Assume for the sake of contradiction that $gaga = g$. Then $aga = e$ by left cancellation. Because $aa = e$ we have $ga = a$ so $g = e$ by right cancellation, a contradiction because we chose g to be an element of G other than e. Therefore $gaga = e$, so ga is an element of G of order 2.

Therefore, for every element $a \in G$ of order 2 different from g we have that $ga \in G$ also has order 2. Since no (a, ga)-pair overlaps with any other pair (because the cosets of $\langle g \rangle$ in G partition G into disjoint sets) we must have an even number of elements of order 2 different from g, so when counting g there must be an odd number.

2.

Let G be a finite abelian group of odd order. Since G is a finite abelian group it is isomorphic to the additive group $\mathbb{Z}_{\left(p_1^{r_1}\right)} \times \ldots \times \mathbb{Z}_{\left(p_1^{r_n}\right)}$ for some primes $p_1, \ldots, p_n$ and positive integers $r_1, \ldots, r_n$, and since G is odd we must have $p_1, \ldots, p_n \neq 2$. Since p_i is odd for all i and $Z_{\left(p_i^{r_i}\right)}$ is cyclic, no element of $\mathbb{Z}_{\left(p_i^{r_i}\right)}$ is it's own inverse, so no element of their product is it's own inverse either. Therefore if we

sum every element of the this abelian group, we can shuffle around the terms to cancel every element against it's own inverse and thereby get a sum of only identities which results in the identity itself. This result can be transferred back to the original group G since they are isomorphic.

3.

Clearly $\langle(2,3)\rangle$ is isomorphic to $\mathbb{Z}_n$, so we should expect the quotient group $\mathbb{Z}_{2n} \times \mathbb{Z}_{3n}/\langle(2,3)\rangle$ to be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_n \cong \mathbb{Z}_{6n}$ (we can collapse the product because the order of each group in the product is relatively prime to the other orders). To prove our hypothesis we must show that the quotient group is cyclic.

Let $G = \mathbb{Z}_{2n} \times \mathbb{Z}_{3n}/\langle(2,3)\rangle$. We choose to represent each coset of $\langle(2,3)\rangle$ by the element witch has either 0 or 1 as it's first element in the pair, i.e. the element of the form $(0,n)$ or $(1,n)$ for some $n \in \mathbb{Z}_{3n}$. This element clearly exists, because we can add and remove $(2,3)$ from our representative as much as we want so by the remainder theorem there must exist some representative with first element r s.t. $0 \leq r < 2$. This element is also unique, because 2 has the same order in $\mathbb{Z}_{2n}$ as 3 in $\mathbb{Z}_{3n}$, so every time the first term is repeated the second term must also repeat, and the each coset contains either a representative with 0 or with 1 as the first term, because 2 only generates the even elements of $\mathbb{Z}_{2n}$.

To prove that G is cyclic, we shall prove that $(1,1)$ generates G. Let $a \in \mathbb{Z}_{3n}$. We want to generate the representative $(0,a)$ and $(1,a)$ from addition and subtraction of $(2,3)$ from a multiple of $(1,1)$, i.e. we must have $(0,a) = m(1,1) + k(2,3)$ for some $m, k \in \mathbb{Z}$, but this is just the linear system of equations:

$$\begin{aligned} m + 2k &= 0 \\ m + 3k &= a \end{aligned}$$

which has the solution $k = a$ and $m = -2a$, and similarly $k = a - 1$ and $m = -2a + 3$ for the equation $(1,a) = m(1,1) + k(2,3)$. Because every element on the form $(0,a)$ and $(1,a)$ can be written on the form $m(1,1) + k(2,3)$ we must have that some element of the cosets $(0,a)\langle(2,3)\rangle$ and $(1,a)\langle(2,3)\rangle$ is a multiple of $(1,1)$, for every $a \in \mathbb{Z}_{3n}$, but we have established that every coset has a representative one of the forms $(0,a)$ or $(1,a)$, so $(1,1)$ is a generator for G.

Problem 2

Let G be a group, and let $\phi_g : G \to G$ be the group isomorphism sending x to gxg^{-1} for all $x, g \in G$.

1.

Let $\Phi_g : G \to \mathrm{Aut}(G)$ be given by $\forall g \in G \quad g \mapsto \phi_g$. We have for all $a, b, x \in G$

$$\begin{aligned}\Phi(ab)(x) &= \phi_{ab}(x) \\ &= (ab)x(ab)^{-1} \\ &= a(bxb^{-1})a^{-1} \\ &= a\phi_b(x)a^{-1} \\ &= \phi_a \circ \phi_b(x)\end{aligned}$$

so $\forall a, b \in G \quad \Phi(ab) = \phi_a \circ \phi_b$, and so Φ is a group homomorphism.

2.

Trivially $\Phi[G]$ is a group because it is the image of a group under a group homomorphism, and it is a subgroup of $\mathrm{Aut}(G)$ because $\forall g \in G \quad \phi_g \in \mathrm{Aut}(G)$.

Let $a \in \mathrm{Aut}(G)$ and let $\phi_g \in \Phi[G]$. Then we have $\forall x \in G$

$$\begin{aligned}a \circ \phi_g \circ a^{-1}(x) &= a(g\, a^{-1}(x) g^{-1}) \\ &= a(g)\, a \circ a^{-1}(x)\, a(g^{-1}) \\ &= a(g)\, x\, a(g^{-1})\end{aligned}$$

but since a is a homomorphism we have $a(g^{-1}) = (a(g))^{-1}$, and so $a(g)\, x\, a(g^{-1}) = \phi_{a(g)}(x)$ for all $x \in G$. Therefore we have $\forall a \in \mathrm{Aut}(G)$, $\forall \phi_g \in \Phi[G] \quad a \circ \phi_g \circ a^{-1} = \phi_{a(g)} \in \Phi[G]$, so $\Phi[g]$ is normal in $\mathrm{Aut}(G)$.

3.

Let $H_1 \sim H_2 \iff \exists g \in G \quad \phi_g(H_1) = H_2$. Trivially $\phi_e(H) = eHe = H$ so $\sim$ is reflexive.

We have $a(bHb^{-1})a^{-1} = abH(ab)^{-1}$ for all subsets $H \subset G$ and $a, b \in G$, so $\phi_a \circ \phi_b(H) = \phi_{ab}(H)$, so if we have $H_1 \sim H_2 \wedge H_2 \sim H_3$, then $\exists g, g' \in G \quad \phi_g(H_1) = H_2 \wedge \phi_{g'}(H_2) = H_3$ so $\phi_{g'} \circ \phi_g(H_1) = \phi_{g'g}(H_1) = H_3$, so $H_1 \sim H_3$ and $\sim$ is transitive.

Let $H_1 \sim H_2$. Then $\phi_g(H_1) = H_2$, but then $\phi_{g^{-1}}(H_2) = H_1$, so $H_1 \sim H_2 \Rightarrow H_2 \sim H_1$ and so $\sim$ is symmetric.

Because $\sim$ is reflexive, transitive and symmetric, it is an equivalence relation.

Problem 3

1.

Let $\sigma = (1,2,5)(4,2,5,6,7)(3,1,7)$ and $\tau = (8,9)$. We see that the orbits of σ aren't disjoint, so by collapsing and simplifying we get $\sigma = (1,4,5,6,7,3,2)$. Let $H = \langle \sigma, \tau \rangle$. Since σ and τ are disjoint permutations we have $|H| = |\sigma| \cdot |\tau| = 7 \cdot 2 = 14$.

Because σ and τ both only have one orbit each, the orbits of $\{1, \ldots, 9\}$ under H are exactly those two orbits, namely $\{1,2,3,4,5,6,7\}$ and $\{8,9\}$.

Because every element of $\{1, \ldots, 7\}$ is in the single orbit of σ there exists for every pair of numbers from that set some power of σ witch maps the first number to the second by the definition of an orbit, so $\langle \sigma \rangle$ acts transitively on $\{1, \ldots, 7\}$.

2.

The orbit $Gp = \{\theta \cdot p \,|\, \theta \in G\}$ of a point $p \neq (0,0)$ is the set of all points with the same euclidean distance to the origin as the point p. This can be thought of as the circumference of the circle with radius $||\vec{r}||_2$ and center at the origin. The isotropy subgroup $G_p = \{\theta \in G \,|\, \theta \cdot p = p\}$ is the set of multiples of full rotations, i.e. the set $\{2\pi k \,|\, k \in \mathbb{Z}\}$.

If $p = (0,0)$ then Gp collapses to just the origin itself because every rotation of the origin around the origin is the origin itself. By the same argument G_p is now the whole of G.

In the case of translations X_t is empty, since no point in the plane is stable under (nontrivial) translation. By the same argument we have $G_p = \{0\}$. The orbit Gp can be geometrically interpreted as the line parallel to the vector $(1,1)$ through the point p.

Problem 4

1.

For the polynomial $x^3 + x + 1$ to be reducible, it has to be divisible by a linear polynomial (either it factors into three linear polynomials or one linear and one quadratic), but if it is divisible by a linear polynomial it must also have a zero, but for no value of x is the polynomial evaluated to zero (just check the two possible values of x). $x^3 + 1$, however, is reducible because it has a zero for $x = 1$, so $x + 1$ divides $x^3 + 1$ and so it can be factored as $x^3 + 1 = (x+1)(x^2 + x + 1)$.

For $x^4+x^3+x^2+1$ to be reducible it has to be divisible by a linear polynomial or an irreducible quadratic polynomial. We can easily check that it is not divisible by a linear polynomial, so then it must be divisible by an irreducible quadratic. There are in total 4 quadratic polynomials in Z_2, namely

$$\begin{aligned} &x^2+x+1\\ &x^2\quad\ +1\\ &x^2+x\\ &x^2 \end{aligned}$$

but only x^2+x+1 is irreducible, however it does not divide $x^4+x^3+x^2+x+1$, so $x^4+x^3+x^2+x+1$ must be irreducible.

2.

We see that because $x^3 \equiv x+1$ we can reduce every polynomial until we have a polynomial of degree 2 or less: factor out x^3 from each term of order ≥ 3 and substitute it with $x+1$ creating two new terms, both of lesser degree. Since there are only a finite number of sub-cubic polynomials in $\mathbb{Z}_2[x]$ (there are only $2^3 = 8$ of them), by our assumption that F is an integral domain and because every finite integral domain is a field, F must be a field.