Problem Set 6
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 1.3

Ex 4 Compute the order of each of the elements in the following groups: (a) S_3 (b) S_4

Proof. Since $S_3 \subseteq S_4$, we only need to find the order of the elements of S_4. The elements that don't have a 4 in them are the elements of S_3.

1) $|\,()\,| = 1$

2) $|\,(12)\,| = |\,(13)\,| = |\,(14)\,| = |\,(23)\,| = |\,(24)\,| = |\,(34)\,| = 2$

3) $|\,(123)\,| = |\,(132)\,| = |\,(142)\,| = |\,(124)\,| = |\,(134)\,| = |\,(143)\,| = |\,(234)\,| = |\,(243)\,| = 3$

4) $|\,(1234)\,| = |\,(1243)\,| = |\,(1324)\,| = |\,(1342)\,| = |\,(1423)\,| = |\,(1432)\,| = 4$

5) $|\,(12)\,(34)\,| = |\,(13)\,(24)\,| = |\,(14)\,(23)\,| = 2$

These are all 24 elements of S_4. All these elements can be proven to have this order by exercise 14, except for group 4, which can be easily checked. $\square$

Ex 13 Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Proof. See next exercise. $\square$

Ex 14 Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Proof. Let $a_i \in G$ be commuting cycles. Claim: $\left(\prod_{i\in I} a_i\right)^n = \prod_{i\in I} a_i^n$. Proof by induction: Let $|I| = 1$. Then the statement is trivial. Suppose the statement holds for all sets of cardinality n, and let $|I| = n+1$. We see that $\left(\prod_{i\in I} a_i\right)^n = \left(a_k \cdot \prod_{i\in I\setminus\{k\}} a_i^n\right) = a_k \cdot$

$\left(\prod_{i\in I\setminus\{k\}} a_i\right)^n = a_k^n \cdot \prod_{i\in I\setminus\{k\}} a_i^n = \prod_{i\in I} a_i^n$. The second equality holds as the a_i commute with each other.

If σ is the product of commuting p-cycles, say a_i, then $\sigma^p = \left(\prod_{i\in I} a_i\right)^p = \prod_{i\in I} a_i^n = \prod_{i\in I} 1 = 1$. This, the order of σ divides p. Since the cycle decomposition is non-trivial, σ is not the identity. Thus, $|\sigma| = p$.

Let $|\sigma| = p$. We can decompose σ into disjoint, and thus commuting, cycles. Now suppose this decomposition contains a cycle a_k of order n, where $n \neq p$. We see that $1 = \sigma^p = \left(\prod_{i\in I} a_i\right)^p = \prod_{i\in I} a_i^p$. Since the a_i's are disjoint, they can't be inverses of each other. Thus it must be that $a_i^p = 1$. This means that the order of a_i divides p. If a_i has order 1, then it must be the identity, so we can remove it and the product is still σ. Thus, each a_i must have order p.

Let $\sigma = (123)(45) \in S_n$ for $n \geq 5$. We see that its decomposition is into disjoint cycles of order 3 and 2. This proves that the result doesn't hold if p is not prime. □

Section 3.2

Ex 14 Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup or order 3.

Proof. Suppose $N \trianglelefteq G$ and $|N| = 3$. Since there are 8 elements of S_4 of order 3 (See Sec 1.3 Ex 4), there must be an element with order 3 that isn't in N, that is to say $xN \neq N$. But we see that $(xN)^3 = x^3N = eN = N$ since N is normal. This means the order of xN is either 1 or 3. It can't be 1, as we assumed that $xN \neq N$. It also can't be 3, as the order of G/N is 8, and thus the order of any element in G/N must divide 8. This proves that there is no normal subgroup of order 3.

Suppose $N \trianglelefteq G$ and $|N| = 8$. Since there are 9 elements of S_4 of order 2 (See Sec 1.3 Ex 4), there must be an element with order 2 that isn't in N, that is to say $xN \neq N$. But we see that $(xN)^2 = x^2N = eN = N$ since N is normal. This means the order of xN is either 1 or 2. It can't be 1, as we assumed that $xN \neq N$. It also can't be 2, as the order of G/N is 3, and thus the order of any element in G/N must divide 3. This proves that there is no normal subgroup of order 8. □

Ex 15 Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \simeq S_{n-1}$.

Proof. Let $I = \{1, \ldots, n\} \setminus \{i\}$, and let $\varphi : G_i \to S_I$ where $\varphi(\sigma) = \sigma\big|_I$, that is, σ restricted to I. We see that this is a permutation of I, as $\sigma(i) = i$. Given a permutation of I, we can extend it to $\{1, \ldots, n\}$, by letting $\sigma(i) = i$. It's easy to see that these two operations are inverses of each other. Thus, φ is a bijection. We also see that $\varphi(\sigma \circ \delta)(x) = (\sigma \circ \delta)\big|_I (x) = \sigma\big|_I \left(\delta\big|_I (x)\right) = \sigma\big|_I (\varphi(\sigma)(x)) = \varphi(\sigma)(\varphi(\delta)(x)) = (\varphi(\sigma) \circ \varphi(\delta))(x)$, where $x \in I$. Thus, φ is a bijective homomorphism, which means that it's a isomorphism. We've proven before that since $|I| = n - 1$, $S_I \simeq S_{n-1}$. Thus, $G_i \simeq S_I \simeq S_{n-1}$. □

Ex 20 If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.

Proof. Let $x \in A \cap B$ and let $g = ab \in AB$. We see that $gxg^{-1} \in A$, as A is normal in G and $x \in A$ and $g \in AB \subseteq G$. We also see that $gxg^{-1} = abx\,(ab)^{-1} = abxb^{-1}a^{-1}$. We see that $bxb^{-1} \in A$, as A is normal in G and $x \in A$ and $b \in B \subseteq G$. Since A is abelian, this means that $abxb^{-1}a^{-1} = aa^{-1}bxb^{-1} = bxb^{-1} \in B$, as $b \in B$ and $x \in B$. Thus, for $g \in AB$ and $x \in A \cap B$, we see that $gxg^{-1} \in A \cap B$. This proves that $A \cap B \trianglelefteq AB$. $\square$

Section 3.3

Ex 1 Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|\mathrm{GL}_n(F) : \mathrm{SL}_n(F)| = q - 1$.

Proof. We know already that $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}$ is a homomorphism where $\ker\det = \mathrm{SL}_n(\mathbb{F})$. Since for any nonzero $f \in \mathbb{F}$, $\det(A) = f$, where A is the matrix with f in the first entry, 1 in the rest of the diagonal, and 0 everywhere else. By definition no element of $\mathrm{GL}_n(\mathbb{F})$ has determinant 0. Thus, $\operatorname{Im}\det = \mathbb{F}^\times$. Thus, by the First Isomorphism Theorem, $\mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F}) \simeq \mathbb{F}^\times$. Since the order of $\mathbb{F}^\times$ is $q-1$, this means that $|\mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F})| = [\mathrm{GL}_n(\mathbb{F}) : \mathrm{SL}_n(\mathbb{F})] = q - 1$. $\square$

Ex 2 Prove all parts of the Lattice Isomorphism Theorem.

Ex 3 Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either

i) $K \leq H$ or

ii) $G = HK$ and $|K : K \cap H| = p$.

Proof. If $K \subseteq H$, then $K \leq H$. Assume that $K \not\subseteq H$. Let $k \in K \setminus H$. Thus, $kH \neq H$. Since $[G : H] = p$, this means that G/H is generated by any nonidentity element of G/H. Thus, $\langle kH \rangle = G/H$. Let $g \in G$. We see that $gH = (kH)^n = k^nH$ for some $n \in \{0, \dots, p-1\}$. This means that $g\,(k^n)^{-1} \in H$, which shows that $gk^{-n} = h$ for some $h \in H$. This means that $g = hk^n \in HK$. This proves that $G = HK$.

Let $\varphi(w(K \cap H)) = wH \in G/H$, where $w \in K$. Let $w(K \cap H) = z(K \cap H)$. Then $wz^{-1} \in K \cap H$. Thus, $wz^{-1}H = H$, as $wz^{-1} \in H$. This means that $wH = zH$. This proves well-definedness. Let $\psi(wH) = w(K \cap H)$, again where $w \in K$. If $wH = zH$, then $wz^{-1} \in H$. wz^{-1} is in K as well, as both w and z are in K. Thus, $wz^{-1} \in H \cap K$, which means that $w(H \cap K) = z(H \cap K)$. This proves well-definedness. It's easy to see that these two functions are inverses. Thus, there is a bijection between the two sets. This proves that $[K : K \cap H] = [G : H] = p$. $\square$

Section 3.4

Ex 1 Prove that if G is an abelian simple group then $G \simeq Z_p$ for some prime p (do not assume G is a finite group).

Proof. Suppose G is abelian and simple. If G has a subgroup, then that subgroup is normal, as G is abelian. Since G is simple, it has no non-trivial normal subgroups, and thus, it can't have any non-trivial subgroups. Let $e \neq g \in G$, which must exist as the definition of simple means that $|G| > 1$. Then $\langle g \rangle$ is a subgoup. Since G has no non-trivial subgroups, then $\langle g \rangle$ must be $\{e\}$ or G itself. Since $g \neq e$, this means that $\langle g \rangle = G$. Thus, G is cyclic. Suppose $|G|$ was not prime. Then $|g|$ is not prime. Let jk be this quantity, where neither is equal to one. This means that $\left(g^j\right)^k = g^{jk} = 1$. Since $|g| = jk$, $g^j \neq e$, as jk is the least quantity with this property. Thus, $|g^j|$ is not 1 and divides k, which means that $1 < |g^j| < jk$. Thus, $1 < |\langle g \rangle| < jk$, which means that $\langle g^j \rangle$ is a proper non-trivial subgroup of G, which is a contradiction. Thus, $|G| = p$ for some prime p. Since G is a cyclic group of order p, this means that $G \simeq Z_p$. □

Ex 2 Exhibit all 3 composition series for Q_8. List the composition factors.

Proof. We see that i, j and k have order 4 and thus generate cyclic groups of order 4. Since $[Q_8 : \langle i \rangle] = 2$, then by additional problem A, $\langle i \rangle$ is normal in Q_8. This group contains $\{-1, 1\}$, which is a group of order 2. Since $[\langle i \rangle : \{-1, 1\}] = 2$, again, $\{-1, 1\}$ must be norman in $\langle i \rangle$. The only subgroups of $\{-1, 1\}$ are trivial, so we're done. This gives the composition series $1 \trianglelefteq \{-1, 1\} \trianglelefteq \langle i \rangle \trianglelefteq Q_8$. Since the index of each part of the chain is 2, the composition factors are all isomorphic to the unique group of order 2. Similarly, this can be done with $\langle j \rangle$ oo $\langle k \rangle$, which give the other two composition series, also with all the composition factors being the group of order 2. □

Additional Problems

Ex A Let H be a subgroup of G and assume that $[G : H] = 2$. Prove that H is a normal subgroup.

Proof. Since $[G : H] = 2$, this means that H has two cosets. Denote them as H and H'. Let $g \in G$. If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then $gH \neq H$, which means that $gH = H'$. By similar reasoning, $Hg = H'$. Thus, $gH = H' = Hg$. Since $gH = Hg$ for all $g \in G$, this proves that H is normal. □

Ex B Recall that a character of a group G is a group homomorphism $\alpha : G \to \mathbb{C}^\times$.

B1) Recall that G acts on $X = G$ by the conjugation action given by $g.x = gxg^{-1}$. Given any $x \in X$, the conjugacy class of x is the orbit $G.x$. Prove that if α is a character, then it is constant on each conjugacy class. That is, if $x_1, x_2 \in X$ are in the same conjugacy class, then $\alpha(x_1) = \alpha(x_2)$.

Proof. B1) Let x_1, x_2 be in the same conjugacy class. That means that $x_1 = g_1.x$ and $x_2 = g_2.x$ for some $x, g_1, g_2 \in G$. This means that $\alpha(x_1) = \alpha(g_1.x) = \alpha\left(g_1 x g_1^{-1}\right) = \alpha(g_1)\,\alpha(x)\,\alpha(x_2)^{-1}$. Since $\mathbb{C}^\times$ is abelian, this means that $\alpha(x_1) = \alpha(x)$. By a similar argument, $\alpha(xstwo) = \alpha(x)$. Thus, $\alpha(x_1) = \alpha(x_2)$.

□

Ex C C1) Prove that every transposition in S_n is an odd element.

C2) If $(a_1, \dots, a_k)$ is a cycle in S_n, please give a method for determining if the cycle is an even or odd element. Of course, please prove your method always works.

Proof. C1) Suppose every transposition was even. Let σ be a permutation. This means that it can be written as a product of transpositions, call them a_i. Since sgn is a homomorphism, this means that $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\prod_{i \in I} a_i) = \prod_{i \in I} \mathrm{sgn}(a_i) = \prod_{i \in I} 1 = 1$. This means that every element of S_n is even. As $\ker \mathrm{sgn} \neq S_n$. Thus, there must be an odd transposition, call it $\tau = (jk)$. Let $\sigma = (mn)$, be an arbitrary transposition. Let λ be the permutation that tranposes m with j and n with k. We see then that $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\lambda \tau \lambda) = \mathrm{sgn}(\lambda)\mathrm{sgn}(\tau)\mathrm{sgn}(\lambda) = \mathrm{sgn}(\tau)\mathrm{sgn}(\lambda)^2 = -1$. Thus, every transposition must be odd.

C2) Such a cycle is odd if k is even and even if k is odd. The proof is that this cycle can be rewritten as $(a_1 a_k)\,(a_1 a_{k-1}) \dots (a_1 a_2)$. This can be verified by seeing that a_1 goes to a_2, and then there are no other cycles containing a_2, so that's the final result. Also, for a_n, where $n \neq k$, it's transposed with a_1, and then immediately transposed with a_{n+1}, which doesn't occur again in any of the other cycles. For a_k, it's transposed in the end with a_1 and that's it. Thus, this is the same cycle. Since sgn is a homomorphism and every transposition has an odd parity, we see that

$$\mathrm{sgn}((a_1 a_2 \dots a_k)) = \mathrm{sgn}((a_1 a_k)\,(a_1 a_{k-1}) \dots (a_1 a_2)) = (-1)^{k-1}$$

Since sgn is a well-defined homomorphism, this is the definitive parity of the cycle. This proves that if k is even, then the parity is odd and vice-versa.

□