MIDTERM II: SOLUTIONS

MATH 3140

1. Let $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{3}]$ is a ring under the ordinary addition and multiplication of real numbers.

Solution. $\mathbb{Z}[\sqrt{3}]$ is a subset of the ring $(\mathbb{R}, +, \cdot)$. Let us first show that $\mathbb{Z}[\sqrt{3}]$ is closed under both $+$ and $\cdot$. Indeed, we have

$$a + b\sqrt{3} + a' + b'\sqrt{3} = (a + a') + (b + b')\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

and

$$(a + b\sqrt{3}) \cdot (a' + b'\sqrt{3}) = (aa' + 3bb') + (ab' + a'b)\sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

Moreover, since $(a + b\sqrt{3}) + (-a' - b'\sqrt{3}) = (a - a') + (b - b')\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, it follows that $(Z[\sqrt{3}], +)$ is a subgroup of $(\mathbb{R}, +)$, and is thus an abelian group. (We are using the fact that if G is a group, and $S \subseteq G$ is a subset, then S is a subgroup if and only if $ab^{-1} \in S$ for all $a, b \in S$.)

To check that $(Z[\sqrt{3}], +, \cdot)$ is a ring, we must check that $(Z[\sqrt{3}], +)$ is an abelian group (which we have done above), that $\cdot$ is associative (this is true since it is true for $\mathbb{R}$), and that the distributive laws hold (this is also true since it is true for $\mathbb{R}$). Thus $(Z[\sqrt{3}], +, \cdot)$ is a ring. $\square$

2. Factor $x^6 + 6 \in \mathbb{Z}_7[x]$ into linear terms in $\mathbb{Z}_7[x]$.

Solution. Let $f(x) = x^6 + 6 \in \mathbb{Z}_7[x]$. By Fermat's Theorem we have $\alpha^6 \equiv 1 \pmod 7$ for all $0 \neq \alpha \in \mathbb{Z}_7$. Thus $f(\alpha) = 0$ for all $0 \neq \alpha \in \mathbb{Z}_7$ (note that this also follows easily by inspection). It follows that $(x - \alpha)$ divides $f(x)$ for all $0 \neq \alpha \in \mathbb{Z}_7$. Consequently

$$x^6 + 6 = (x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)q(x) \in \mathbb{Z}_7[x],$$

for some $q(x) \in \mathbb{Z}_7[x]$. For reasons of degree, $\deg q(x) = 1$. By considering the coefficient of x^6, it is clear that $q(x) = 1$. Thus

$$x^6 + 6 = (x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6) \in \mathbb{Z}_7[x].$$

$\square$

3. Let F be a field and let K be a subset of F with at least two elements. Prove that K is a subfield of F if for any $a, b \in K$ with $b \neq 0$, then both $a - b$ and ab^{-1} are in K.

Date: November 16, 2009.

Solution. To fix notation, we have the field F given by the collection $(F, +, \cdot)$. Consider the subset K of the group $(F, +)$. I claim that $a - b \in K$ for all $a, b \in K$. Indeed, this is true by assumption unless $b = 0$, in which case $a - b = a \in K$. It follows that $(K, +)$ is a subgroup of $(F, +)$, and hence is an abelian group.

Now consider $K^* = K - \{0\}$ and $F^* = F - \{0\}$. We know that $(F^*, \cdot)$ is a group. By assumption K^* is a *non-empty* subset of this group with the property that $ab^{-1} \in K$ for all $a, b \in K^*$. In fact, since F is an integral domain, it must be that $ab^{-1} \in K^*$ for all $a, b \in K^*$. Thus $(K^*, \cdot)$ is a subgroup of $(F^*, \cdot)$.

It is also true that K is closed under the operation $\cdot$. Indeed, since K^* is closed under $\cdot$, it remains only to observe that $a \cdot 0 = 0 \cdot a = 0 \in K$ for all $a \in K$ (recall that $0 \in K$ since $(K, +) \leq (F, +)$).

To check that $(K, +, \cdot)$ is a ring, we must check that $(K, +)$ is an abelian group (which we have done in the first paragraph), that $\cdot$ is associative (this is true since it is true for F), and the distributive laws hold (this is also true since it is true for F). Thus K is a subring of F. It follows that K is a commutative ring.

Now since K^* is a subgroup of F^* it contains the multiplicative identity $1 \neq 0$ and every element $a \in K^*$ has a multiplicative inverse $a^{-1} \in K^*$. Thus K is a subfield of F. □

4. True or false. If true, prove the statement. If false, provide a counter example.
   (a) If $d \mid |G|$ then there exists a $g \in G$ such that $|g| = d$.
   (b) Suppose R is a ring and $a, b \in R$. If $ab = 0$ then either $a = 0$ or $b = 0$.

Solution. (a) and (b) are both false. For (a) consider the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then the number 4 divides $|G| = 4$. On the other hand, every element of G has order at most two. For (b) consider the ring $\mathbb{Z}_4$. We have $[2][2] = [4] = [0] \in \mathbb{Z}_4$, and $[2] \neq [4]$. □

5. Let G be a group. Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. To show G is abelian, we must show that given $g_1, g_2 \in G$, then

$$g_1 g_2 = g_2 g_1.$$

To begin, since the group $G/Z(G)$ is cyclic, it has a generator $[g] \in G/Z(G)$ for some $g \in G$. It follows that there are integers n_1, n_2 such that

$$[g_1] = [g]^{n_1} \text{ and } [g_2] = [g]^{n_2}.$$

We can rewrite this by saying that there exists $z_1, z_2 \in Z(G)$ such that $g_1 = g^{n_1} z_1$ and $g_2 = g^{n_2} z_2$. Then

$$g_1 g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_2} z_2 g^{n_1} z_1 = g_2 g_1$$

since by definition z_1, z_2 commute with all elements of G, and g commutes with itself. □

6. An element of a of a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$. Show that if $a \in R$ is nilpotent, then $1 - a$ has a multiplicative inverse in R.

Solution. Using the condition $a^n = 0$, we have

$$(1 - a)(1 + a + a^2 + \ldots + a^{n-1}) = 1 - a^n = 1.$$

Thus $1 + a + a^2 + \ldots + a^{n-1}$ is the multiplicative inverse of $(1 - a)$. $\square$

7. Show that A_n is a simple group for $n \geq 5$.

Solution. We break this problem into several parts.
Claim (a): A_n contains every 3-cycle if $n \geq 3$.

Proof. Let $(a_1, a_2, a_3) \in S_n$ be a 3-cycle. Since $(a_1, a_2, a_3) = (a_1, a_2)(a_3, a_2)$ it follows from the definition that $(a_1, a_2, a_3) \in A_n$. $\square$

Claim (b): A_n is generated by the 3-cycles.

Proof. Let $\sigma \in A_n$ be a nontrivial element. By definition there is an expression of σ

$$\sigma = \tau_1 \tau_2 \cdots \tau_{2n-1} \tau_{2n}$$

as a composition of transpositions $\tau_1, \ldots, \tau_{2n}$ for some $n \in \mathbb{N}$. Since there are n-pairs of transpositions in the expression, the claim will follow if we can show that for any transpositions $\tau, \hat{\tau} \in S_n$ with $\tau \neq \hat{\tau}$, then $\tau\hat{\tau}$ is a composition of 3-cycles.

To prove this, suppose $\tau = (a_1, a_2)$ and $\hat{\tau} = (a_3, a_4)$. There are two cases to consider:

(1) If $a_i \neq a_j$ for $i, j \in \{1, 2, 3, 4\}$ and $i \neq j$, then $(a_1, a_2)(a_3, a_4) = (a_1, a_3, a_2)(a_1, a_3, a_4)$.
(2) Otherwise $a_i = a_j$ for some $i \neq j$, and we can assume without loss of generality that $a_2 = a_4$. Then we have $(a_1, a_2)(a_3, a_2) = (a_1, a_2, a_3)$.

Thus $\tau\hat{\tau}$ is a composition of 3-cycles, completing the proof of Claim (b). $\square$

Claim (c): Fix $r, s \in \{1, \ldots, n\}$ with $r \neq s$. If $n \geq 3$, then A_n is generated by the set of 3-cycles $\{(r, s, i) : 1 \leq i \leq n\}$.

Proof. After some manipulation, one can establish the identities:

(i) $(r, s, i)^2 = (s, r, i)$,
(ii) $(r, s, j)(r, s, i)^2 = (r, i, j)$,
(iii) $(r, s, j)^2(r, s, i) = (s, i, j)$,
(iv) $(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i) = (i, j, k)$.

Since every 3-cycle is of the form of one of those above, it follows that A_n is generated by the set of 3-cycles $\{(r, s, i) : 1 \leq i \leq n\}$. $\square$

Claim (d): Suppose $n \geq 3$. Let $N \lhd A_n$ be a normal subgroup. If N contains a 3-cycle then $N = A_n$.

Proof. Suppose N contains a 3-cycle σ. Then $\sigma = (r, s, i)$ for some choice of $r, s, i \in \{1, \ldots, n\}$. Observe (after some manipulation) that for any $j \neq i \in \{1, \ldots, n\}$ we have

$$((r, s)(i, j))\,(r, s, i)^2\,((r, s)(i, j))^{-1} = (r, s, j).$$

The expression on the left in in N since it is a conjugate of an element of N. Thus N contains the set $\{(r, s, j) : 1 \leq j \leq n\}$. By virtue of Claim (c), it follows that $N = A_n$. $\square$

Claim (e): Suppose $n \geq 5$. If $N \lhd A_n$ is a non-trivial normal subgroup, then N contains a 3-cycle.

Proof. We will do this in a case by case analysis. The first step is to show that if $N \lhd A_n$ is a non-trivial normal subgroup, then one of the following cases holds:
CASE I: There exists $\sigma \in N$ that can be written as a disjoint product of the form $\sigma = \mu(a_1, \dots, a_r)$ for some $r \geq 4$.
CASE II: There exists $\sigma \in N$ that can be written as a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$.
CASE III: There exists $\sigma \in N$ that can be written as a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$, with μ a disjoint product of transpositions.
CASE IV: There exists $\sigma \in N$ that can be written as a disjoint product of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, with μ a disjoint product of transpositions.

To see that one of these cases must hold, consider the fact that any non-trivial $\sigma \in S_n$ can be written as a product of disjoint cycles

$$\sigma = \sigma_1 \dots \sigma_m$$

for some $m \in \mathbb{N}$. Since disjoint cycles commute, we may reorder so that the length of the cycles is non-decreasing. The fact that one of the cases above must hold is then obvious.

Now we will show that in each case above, N contains a 3-cycle. For Case I, consider the expression $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$. This is in N since $(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is a conjugate of an element of N. On the other hand, after some algebra, one has

$$\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} = (a_1, a_3, a_r),$$

so that N contains a 3-cycle.

For Case II, consider the expression $\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}$. Again this is clearly in N, and after some algebra one has

$$\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1} = (a_1, a_4, a_2, a_6, a_3).$$

Thus N contains a cycle of length five, and so by Case I, it also contains a cycle of length three.

For Case III, one has

$$\sigma^2 = (a_1, a_3, a_2)$$

using the fact that μ^2 is the identity (it is the product of disjoint transpositions). Thus N contains a 3-cycle.

Finally, for Case IV, consider $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$. Some algebra shows that this is equal to $(a_1, a_3)(a_2, a_4)$. We call this permutation α, which as above, is in N. Now let $\beta = (a_1, a_3, i)$ for some $i \in \{1, \dots, n\} - \{a_1, \dots, a_n\}$. Then

$$\beta^{-1}\alpha\beta\alpha = (a_1, a_3, i),$$

which again is in N for the same reason. Thus N contains a 3-cycle. □

Let us conclude by showing that A_n is simple for $n \geq 5$. Let $N \lhd A_n$ be a non-trivial normal subgroup of A_n. In Claim (e) we showed that such a subgroup must contain a 3-cycle. In Claim (d) we showed that if N contains a 3-cycle, then it is equal to A_n. This proves that the only normal subgroups of A_n are the trivial subgroup and A_n. Thus A_n is simple. □