MATH 120 Final. Fri Jun 8 2012.

1.

2. (a) (2 points) Let R be a ring. Give a definition of an ideal of R.

   (b) (6 points) Let I be an ideal of R. Show that

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some integer } n \geq 1\}$$

   is an ideal of R.

   (c) (4 points) Give an example of a ring R and an ideal I where $\sqrt{I} \neq I$.

Solution:

(a) We say that $I \subseteq R$ is an ideal of R if it is both closed under addition and under scaling by an element of R. That is for all $a, b \in I$ and $r \in R$ we must have $a + b \in I$ and $ra \in I$.

(b) Let $a, b \in \sqrt{I}$ and $r \in R$. First we prove $a + b \in \sqrt{I}$. By definition of $\sqrt{I}$ there exist integers n and m such that a^n and b^m are elements of I. Then we consider the binomial expansion of $(a + b)^{n+m}$

$$(a + b)^{n+m} = \sum_{i=0}^{n+m} a^{n+m-i} b^i$$

Since either $i \geq m$ or $n + m - i \geq n$ each term of the summation is an element of I and therefore $(a + b)^{n+m} \in I$ which implies $a + b \in \sqrt{I}$.

Next we show $ra \in \sqrt{I}$. Let us consider $(ra)^n = r^n a^n$, since $a^n \in I$ we have $r^n a^n \in I$ and therefore $(ra)^n \in I$ which implies $ra \in I$.

(c) Let us consider $R = \mathbb{Z}$ and $I = 4\mathbb{Z}$ the ideal of all multiples of 4. We have that $2 \in \sqrt{I}$ since $2^2 = 4$, but $2 \notin I$.

3. Let $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Define $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$.

   (a) (3 points) Prove that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$

   (b) (9 points) Prove that $\mathbb{Z}[\omega]$ is an Euclidean domain with respect to the norm function $N(z) = z\bar{z}$.

Solution:

(a) We will show $\mathbb{Z}[\omega]$ is a subgroup and it is closed under multiplication. First we notice $0 = 0 + 0\omega$ and $1 = 1 + 0\omega$ are elements of $\mathbb{Z}[\omega]$. Next we show that $\mathbb{Z}[\omega]$ is closed under addition and additive inverse. For this we note that if $a_1 + a_2\omega$ and $b_1 + b_2\omega$ are two elements of $\mathbb{Z}[\omega]$ where $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2$. Then we have $(a_1 + a_2\omega) + (b_1 + b_2\omega) = (a_1 + b_1) + (a_2 + b_2)\omega$ and since $a_i + b_i \in \mathbb{Z}$ for

$i = 1, 2$ we have that the sum is an element of $\mathbb{Z}[\omega]$. Similarly we notice that $-(a_1 + a_2\omega) = (-a_1) + (-a_2)\omega$ which is also an element of $\mathbb{Z}[\omega]$.
Next we prove that $\mathbb{Z}[\omega]$ is closed under multiplication. For this we first notice that ω satisfies $\omega^3 = 1$ and thus it satisfies $\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1) = 0$. Since $\omega \neq 1$ we must have $\omega^2 + \omega + 1 = 0$ and therefore $\omega^2 = -1 - \omega$. Now given $a_1 + a_2\omega$ and $b_1 + b_2\omega$ as above we have

$$\begin{aligned}(a_1 + a_2\omega)(b_1 + b_2\omega) &= a_1b_1 + (a_1b_2 + a_2b_1)\omega + (a_2b_2)\omega^2 \\ &= a_1b_1 + (a_1b_2 + a_2b_1)\omega + (a_2b_2)(-1 - \omega) \\ &= a_1b_1 - a_2b_2 + (a_1b_2 + a_2b_1 - a_2b_2)\omega\end{aligned}$$

thus $\mathbb{Z}[\omega]$ is also closed under multiplication and therefore a subring of $\mathbb{C}$.

(b) Let us consider $\mathbf{a} = a_1 + a_2\omega$ and $\mathbf{b} = b_1 + b_2\omega$. We want to find $\mathbf{q}$ in $\mathbb{Z}[\omega]$ such that we can write

$$\mathbf{a} = \mathbf{b}\mathbf{q} + \mathbf{r}$$

with $N(\mathbf{r}) < N(\mathbf{b})$. We will consider $\mathbf{a}$, $\mathbf{b}$ in $\mathbb{C}$ and then the division equation as above is equivalent to have

$$\mathbf{r} = \mathbf{b}\left(\frac{\mathbf{a}}{\mathbf{b}} - \mathbf{q}\right)$$

We can extend N to a norm in $\mathbb{C}$ and thus if we can find $\mathbf{q}$ such that $N(\frac{\mathbf{a}}{\mathbf{b}} - \mathbf{q}) < 1$ then this will imply $N(\mathbf{r}) < N(\mathbf{b})$ and we would be done. First we notice that we can write $\frac{\mathbf{a}}{\mathbf{b}}$ as $c_1 + c_2\omega$ where c_1 and c_2 are rational numbers. Indeed we have

$$\begin{aligned}\frac{1}{\mathbf{b}} &= \frac{b_1 + b_2\bar{\omega}}{(b_1 + b_2\omega)(b_1 + b_2\bar{\omega})} \\ &= \frac{b_1 + b_2\bar{\omega}}{b_1^2 - b_1b_2 + b_2^2} \\ &= \frac{1}{b_1^2 - b_1b_2 + b_2^2}(b_1 + b_2(-1 - \omega)) \\ &= \frac{1}{b_1^2 - b_1b_2 + b_2^2}(b_1 - b_2 - b_2\omega)\end{aligned}$$

And thus when multiplying by $\mathbf{a}$ we will get an element of $\mathbb{Z}[\omega]$ divided by $b_1^2 - b_1b_2 + b_2^2$. Next we choose integer numbers q_1 and q_2 such that $|c_i - q_i| \leq \frac{1}{2}$. Then the complex number $\frac{\mathbf{a}}{\mathbf{b}} - \mathbf{q} = (c_1 - q_1) + (c_2 - q_2)\omega$ has norm $(c_1 - q_1)^2 - (c_1 - q_1)(c_2 - q_2) + (c_2 - q_2)^2$ which is strictly less than 1 since $|c_i - q_i| \leq \frac{1}{2}$.

4. Let T be a subgroup of a group G. Recall the normalizer subgroup defined to be

$$N_G(T) = \{g \in G | gtg^{-1} \in T \ \forall t \in T\}$$

You may assume without a proof that this is a group.

(a) (6 points) Prove that T is a normal subgroup of $N_G(T)$.

(b) (6 points) Let k be a field with more than 2 elements. In the case where $G = \mathrm{GL}_2(k)$ and T is the subgroup of diagonal matrices

$$\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix}$$

with $t_1, t_2 \neq 0$, identify the quotient group $N_G(T)/T$.

Solution:

(a) First we notice that T is a subgroup of $N_G(T)$. This is because for any two elements t_1 and t_2 of T we have $t_1 t_2 t_1^{-1} \in T$ and thus $t_1 \in N_G(T)$ and we have $T \subseteq N_G(T)$. Next we prove that T is normal in $N_G(T)$. Consider $n \in N_G(T)$ and $t \in T$. By definition of $N_G(T)$ we have $ntn^{-1} \in T$, thus $nTn^{-1} \subseteq T$ and this implies that T is normal in $N_G(T)$.

(b) First we identify $N_G(T)$. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

be a matrix in $N_G(T)$. Then for all t_1 and t_2 we must have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \in T$$

Mutiplying this matrices we obtain

$$\frac{1}{ad - bc} \begin{bmatrix} t_1 ad - t_2 bc & (t_2 - t_1)ab \\ (t_1 - t_2)cd & -t_1 bc + t_2 ad \end{bmatrix} \in T$$

since this must hold for all t_1 and t_2 we must conclude that $ab = 0$ and $cd = 0$. Since A must be in $\mathrm{GL}_2(k)$ either we have $a = d = 0$ and $b, c \neq 0$ or $b = c = 0$ and $a, d \neq 0$. Now we look for the cosets of T in $N_G(T)$. We note that

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in T$$

and thus corresponds to the identity coset T. Next, the matrices

$$\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & b \end{bmatrix}$$

and this implies that the only coset besides the identity is the coset corresponding to the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Since we only have two elements in $N_G(T)/T$ the group should be isomorphic to $\mathbb{Z}/2\mathbb{Z}$.