MA3201 Homework 2

Tan Yee Jian (A0190190L)

February 12, 2021

Problem 1

We denote $Ann_R(I)$ as A. We want to show that A is a subring of R and $RA \subseteq A \supseteq AR$.

Solution

Proof. A is a subring:
First, A is a subgroup of R since $0 \in A \neq \emptyset$ and for any $a_1, a_2 \in A$, we have

$$(a_1 - a_2)x = a_1x - a_2x = 0 - 0 = 0 \implies (a_1 - a_2) \in A.$$

Secondly, A is closed under multiplication:

$$a_1a_2x = a_1(0) = 0 \implies a_1a_2 \in A.$$

A is a (two-sided) ideal:
For any $\sum r_k a_k \in RA, r_k \in R, a_k \in A, x \in I$,

$$\begin{aligned}
(\sum r_k a_k)x &= \sum r_k(a_k x) && \text{(distributivity, associativity)}\\
&= \sum r_k(0) = 0 \implies RA \subseteq A && (A \text{ annihilates } I)
\end{aligned}$$

For any $\sum a_k r_k \in AR, r_k \in R, a_k \in A, x \in I$,

$$\begin{aligned}
(\sum a_k r_k)x &= \sum a_k(r_k x) && \text{(distributivity, associativity)}\\
&= \sum a_k x_k = 0 \implies AR \subseteq A. && (x_k \in I \text{ for all } k \text{ since } I \text{ is ideal})
\end{aligned}$$

□

Problem 2

1. Show that every element in $R \setminus M$ is a unit.

   Proof. Suppose otherwise, let $r \in R \setminus M$ be a non-unit. Then $r \in (r) \subseteq M'$ for some maximal ideal M'. Since there is only one unique maximal ideal in R, we have $r \in M' = M$, a contradiction. □

2. Show that if the set of nonunits in R is an ideal, then R is local.

   Proof. Let an arbitrary maximal ideal M be given, we show uniqueness. Denote the set of all non-units be I.

   Since M as a (non-trivial) maximal ideal cannot contain any units, we must have $M \subseteq I$ since I collects all the nonunits. On the other hand, since I is a proper ideal (witnessed by $1 \notin I$), we have $M = I \subsetneq R$ by the maximality of M. Therefore R is local with the unique maximal ideal I. □

Problem 3

1. Show the preimage of a prime ideal under a ring homomorphism $\phi : R \to S$ is either the whole ring or a prime ideal.

   Proof. Since the ideals in the R containing $\ker\phi$ and the ideals in $\phi(R) \cong R/\ker(\phi)$ are in one-one correspondence (by the Correspondence Theorem), the preimage of an ideal is also an ideal.

   We just need to show the "primeness" of the preimage when it is not the whole ring: that given any $ab \in \phi^{-1}(P) \neq R$ where P is a prime ideal in S, either $a \in \phi^{-1}(P)$ or $b \in \phi^{-1}(P)$.

   Note that since $ab \in \phi^{-1}(P)$,

   $$\phi(ab) \in P \implies \phi(a)\phi(b) \in P \implies \phi(a) \in P \wedge \phi(b) \in P.$$

   Since

   $$\phi^{-1}(P) \subsetneq R \implies P \subsetneq \phi(R) \implies \phi(a), \phi(b) \in P \subseteq \phi(R) \implies a \in \phi^{-1}(P) \text{ or } b \in \phi^{-1}(P).$$

   Therefore $\phi^{-1}(P)$ is a prime ideal. □

2. If a ring homomorphism $\phi : R \to S$ is surjective, then the preimage of a maximal ideal in S is a maximal ideal in R.

   Proof. Suppose otherwise, and let $N \subsetneq S$ be the maximal ideal in S such that its preimage is not maximal in R. In particular, $\phi^{-1}(N)$ is contained in some maximal ideal M, where $\phi^{-1}(N) \subsetneq M \subsetneq R$. Consider the image under ϕ:

   $$\phi^{-1}(N) \subsetneq M \implies N \subsetneq \phi(M)$$

   but N is maximal in S. This implies $\phi(M) = S$, and since N is a strict subset of $\phi(M)$, $\phi(M)$ is a non-trivial ring. Any element in $R - M$ cannot be mapped to zero (otherwise $M = R$ a contradiction), but by surjectivity,

   $$\phi(M) = S = \phi(R) \implies R \setminus M = \emptyset$$

   contradicting the (proper) maximality of M. □

Problem 4

1. *Proof.* Let us denote the embedding from the ring R to its localization $D^{-1}R$ as $\varphi : r \mapsto \frac{r}{1}$, and define $R'(\cong R) = \varphi(R) \subset D^{-1}R$.

   I claim that $I = \varphi^{-1}(R' \cap J)$ is an ideal in R and I generates J, ie $(D^{-1}R)\varphi(I) = J$.

   (a) $I \subseteq R$ is an ideal in R.
   <u>I is a subgroup of R</u>: First, note that $\frac{0}{1} \in R' \cap J \implies 0 \in I \neq \emptyset$.
   Let $a, b \in I = \varphi^{-1}(R' \cap J)$ be given. Then $\varphi(a), \varphi(b) \in R' \cap J$. Since R', J are Abelian subgroups of the localization,

   $$\begin{aligned} \varphi(a) - \varphi(b) \in R' \ \wedge \ \varphi(a) - \varphi(b) \in J &\implies \varphi(a) - \varphi(b) \in R' \cap J \\ &\implies \varphi(a - b) \in R' \cap J \\ &\implies (a - b) \in \varphi^{-1}(R' \cap J) = I. \end{aligned}$$

   <u>I is a subring of R</u>: Let $a, b \in I = \varphi^{-1}(R' \cap J)$ be given. Then $\varphi(a), \varphi(b) \in R' \cap J$. Since R', J are Abelian subgroups of the localization,

   $$\begin{aligned} \varphi(a)\varphi(b) \in R' \ \wedge \ \varphi(a)\varphi(b) \in J &\implies \varphi(a)\varphi(b) \in R' \cap J \\ &\implies \varphi(ab) \in R' \cap J \\ &\implies (ab) \in \varphi^{-1}(R' \cap J) = I. \end{aligned}$$

This shows I is also closed under multiplication and hence is a subring of R.
I is an ideal of R: Given any $r \in R, a \in I$,

$$\begin{aligned}\varphi(ra) &= \frac{ra}{1} \\ &= \frac{r}{1} \cdot \frac{a}{1} \\ &\in R'J && (\varphi(a) = \frac{a}{1} \in (R' \cap J)) \\ &\subseteq J && (J \text{ is an ideal}).\end{aligned}$$

And since $ra \in RI \subseteq R$, we must have $\varphi(ra) \in (R' \cap J) \implies (ra) \in I$.

(b) I generates J, ie. $(D^{-1}R)\varphi(I) = (D^{-1}R)(R' \cap J) = J$.
Here is a useful characterization: $I = \varphi^{-1}(R' \cap J) = \{r \in R | \frac{r}{1} \in J\}$.
($\supseteq$): Given any $\frac{r}{d} \in J$ where $r \in R, d \in D$, we have $\frac{1}{d} \cdot \frac{r}{1} \in (D^{-1}R)(R' \cap J)$.
($\subseteq$): This is trivial since $(R' \cap J) \subseteq J$, which implies $(D^{-1}R)(R' \cap J) \subseteq (D^{-1}R)J \subseteq J$.

□

2. Show if R is a PID, then $D^{-1}R$ is a PID.

Proof. We show any ideal $J \subset D^{-1}R$ is principal. Let J be given, and by the previous part, we have a I that generates it. Concretely,

$$\begin{aligned}J &= (D^{-1}R)\varphi(I) \\ &= (D^{-1}R)\varphi(Rr) && \text{for some } r \in I \text{ since } R \text{ is a PID} \\ &= (D^{-1}R)\varphi(R)\varphi(r) && \text{homomorphism} \\ &= (D^{-1}R)\frac{r}{1} && \varphi(R) \subseteq (D^{-1}R) \\ &= (\frac{r}{1}).\end{aligned}$$

Thus J is also a principal ideal, and $D^{-1}R$ a PID.

□

Problem 5

We first show that

Lemma. $N(ab) = N(a)N(b) \forall a, b \in \mathbb{Z}[\sqrt{2}]$.

Proof. For $a, b, c, d \in \mathbb{Z}$,

$$\begin{aligned}N[(a + b\sqrt{2})(c + d\sqrt{2})] &= N(ac + 2bd + (ad + bc)\sqrt{2}) \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= (ac)^2 + 4(bd)^2 - 2(ad)^2 - 2(bc)^2 \\ &= (a^2 - 2b^2)(c^2 - 2d^2) \\ &= N[(c + d\sqrt{2})(a + d\sqrt{2})].\end{aligned}$$

□

Now we show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain.

Proof. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$. We want to show that there exist $q, r \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = q\beta + r$, where $r = 0$ or $N(r) < N(\beta)$.

Let $p, q \in \mathbb{Q}$ be such that

$$\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{2}] = p + q\sqrt{2}.$$

We can then choose $m, n \in \mathbb{Z}$ such that

$$|m-p| \le 1/2, |n-q| \le 1/2.$$

Now

$$\begin{aligned}
\alpha &= \beta(p+q\sqrt{2}) \\
&= \beta(m+n\sqrt{2}+(p-m)+(q-n)\sqrt{2}) \\
&= (m+n)\beta + ((p-m)+(q-n)\sqrt{2})\beta \\
&= q\beta + r
\end{aligned}$$

is as desired since

$$\begin{aligned}
N(r) &= N[(p-m)+(q-n)\sqrt{2}] \cdot N(\beta) && \text{(lemma)} \\
&\le (1/2)^2 \cdot N(\beta) && (|m-p| \le 1, |n-q| \le 1/2) \\
&= \frac{1}{2} N(\beta) \\
&\le N(\beta). && (N(\beta) \ge 0)
\end{aligned}$$

Thus $\mathbb{Z}[\sqrt{2}]$ with the norm defined is an Euclidian Domain. $\square$