Problem Set 2
Abstract Algebra II

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 7.5

Ex 2 Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).

Proof. Let F be the field of fractions of R, and let $\varphi : D^{-1}R \to F$, where $\varphi(\frac{r}{d}) = \frac{r}{d}$. To prove that this is well-defined, suppose that $\frac{r}{d} = \frac{s}{f}$ in $D^{-1}R$. Then we know that $rf = sd$ in R, which means that $\frac{r}{d} = \frac{s}{f}$ in F as well. This proves that φ is well-defined. We see that $\varphi(\frac{r}{d} + \frac{s}{f}) = \frac{r}{d} + \frac{s}{f} = \varphi(\frac{r}{d}) + \varphi(\frac{s}{f})$ and that $\varphi(\frac{r}{d} \cdot \frac{s}{f}) = \varphi(\frac{rs}{df}) = \frac{rs}{df} = \frac{r}{d} \cdot \frac{s}{f} = \varphi(\frac{r}{d})\varphi(\frac{s}{f})$, which prove that φ is a ring homomorphism.

Let $\varphi(\frac{r}{d}) = \varphi(\frac{s}{f})$. This means that $\frac{r}{d} = \frac{s}{f}$ in F, which means that $rf = sd$ in R, and finally that $\frac{r}{d} = \frac{s}{f}$ in $D^{-1}R$. This proves that that φ is an injective homomorphism, meaning that $D^{-1}R$ is isomorphic to a subring of F. Since F is an integral domain, so must $D^{-1}R$. $\square$

Ex 3 Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof. Every field must contain at least 0 and 1. Since a field is closed under addition, this smallest subfield must contain the additive subgroup generated by 1. This means the smallest field contains either $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (it must be prime as $\mathbb{Z}/n\mathbb{Z}$ has zero divisors). If it contains $\mathbb{Z}$, then it must contain all the inverses of $\mathbb{Z}$, and thus must be $\mathbb{Q}$. If it contains $\mathbb{Z}/p\mathbb{Z}$, then we were done, as $\mathbb{Z}/p\mathbb{Z}$ is already a field. This proves the statement. $\square$

Ex 5 If F is a field, prove that the field of fractions of $F[[x]]$ (the ring of formal power series in the indeterminate x with coefficients in F) is the ring $F((x))$ of Laurent series. Show the field of fractions of the power series ring $\mathbb{Z}[[x]]$ is properly contained in the field of Laurent series $\mathbb{Q}((x))$.

Proof. [Incomplete. I was very sick over the weekend.] $\square$

Ex 6 Prove that the real numbers, $\mathbb{R}$, contain a subring A with $1 \in A$ and A maximal under inclusion with respect to the property that $\frac{1}{2} \notin A$. [Use Zorn's Lemma]

Proof. Let S be the set of all subrings of $\mathbb{R}$ which contain 1 but do not contain $\frac{1}{2}$. Since $\mathbb{Z}$ is a ring which contains 1 but does not contain $\frac{1}{2}$, we see that S is nonempty. Let $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ be a chain in S, and let $A = \cup_{i \in \mathbb{N}} A_i$. We have proved previously that A is a subring of R. Note that $1 \in A$, as $1 \in A_1$. If $\frac{1}{2} \in A$, then that means that $\frac{1}{2} \in A_i$ for some i. This is a contradiction, so $\frac{1}{2} \notin A$. This proves that $A \in S$, and we see that A is an upper bound for this given chain. By Zorn's Lemma, S contains a maximal element, which completes the proof. $\square$

Section 7.6

Ex 1 An element $e \in R$ is called an idempotent if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \simeq Re \times R(1-e)$. Show that e and $1-e$ are identites for the subrings Re and $R(1-e)$ respectively.

Proof. We see that $Re + Re = (R+R)e = Re$, that $R \cdot Re = RRe = Re$, and that $Re \cdot R = ReR = RRe = Re$, which proves that Re is a two-sided ideal. Similarly, $R(1-e) + R(1-e) = (R+R)(1-e) = R(1-e)$, $R \cdot R(1-e) = RR(1-e) = R(1-e)$, and $R(1-e) \cdot R = R(1-e)R = R(R-eR) = R(R-Re) = RR(1-e) = R(1-e)$, which proves that $R(1-e)$ is a two-sided ideal.

Suppose $x \in Re \cap R(1-e)$. This means that $r_1 e = r_2(1-e)$ for some $r_1, r_2 \in R$. This would mean that $r_1 e = r_2 - r_2 e$. Multiplying on the right by e, gets us that $r_1 e^2 = r_2 e - r_2 e^2$, which means that $r_1 e = r_2 e - r_2 e = 0$, and thus that $x = 0$. This shows that $Re \cap R(1-e)$ is trivial. If we let $r \in R$, then we see that $re + r(1-e) = re + r - re = r$, and thus that $Re + R(1-e) = R$. This proves using the recognition theorems for internal direct products that $\varphi : Re \times R(1-e) \to R$ where $\varphi(a,b) = a+b$ is a group isomorphism over the additive part of the rings.

Now let $(r_1 e, r_2(1-e))$ and $(r_3 e, r_4(1-e))$ be elements of $Re \times R(1-e)$. We see that $\varphi((r_1 e, r_2(1-e))(r_3 e, r_4(1-e))) = \varphi((r_1 r_3 e, r_2 r_4(1-e))) = r_1 r_3 e + r_2 r_4 (1-e) = r_1 r_3 e^2 + r_2 r_4 (1-e)^2 = r_1 e r_3 e + r_1 r_4 (e - e^2) + r_3 r_2 (e - e^2) + r_2(1-e) r_4 (1-e) = (r_1 e + r_2(1-e))(r_3 e + r_4(1-e)) = \varphi((r_1 e, r_2(1-e)))\varphi((r_3 e, r_4(1-e)))$, which shows that φ respects the multiplicative structure of the rings as well, and thus that φ is a ring isomorphism.

We see that for all $re \in Re$ that $ree = re^2 = re$ and that $ere = ree = re^2 = re$, which proves that e is the identity in Re. We also see that for all $r(1-e) \in R(1-e)$ that $r(1-e)(1-e) = r(1-e)^2 = r(1-2e+e^2) = r(1-2e+e) = r(1-e)$ and similarly for the other side. This proves that $1-e$ is the identity for $R(1-e)$. $\square$

Ex 2 Let R be a finite Boolean Ring with identity $1 \neq 0$. Prove that $R \simeq \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

Proof. This will be a proof by induction. If $|R| = 2$, then $R \simeq \mathbb{Z}/2\mathbb{Z}$ trivially (as it's the only ring with two elements). Now let $|R| = n+1$ and assume that every boolean ring with cardinality between 2 and n is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some k. Now, since

$|R| > 2$ then there exists an element e not equal to 0 or 1 where $e^2 = e$, by definition of being a Boolean Ring. By the previous exercise, this means that $R \simeq Re \times R(1-e)$. We see that Re and $R(1-e)$ are not zero ideals, as that would mean that $e = 0$ or $e = 1$ respectively. Thus, the cardinality of Re and $R(1-e)$ is less than $n+1$. By the induction hypothesis, this means that $Re \simeq (\mathbb{Z}/2\mathbb{Z})^k$ and $R(1-e) \simeq (\mathbb{Z}/2\mathbb{Z})^m$ for some m and k. Thus, $R \simeq Re \times R(1-e) = (\mathbb{Z}/2\mathbb{Z})^k \times (\mathbb{Z}/2\mathbb{Z})^m = (\mathbb{Z}/2\mathbb{Z})^{k+m}$. This proves the statement. $\square$

Ex 5 Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs: $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

a) Show that the Chinese Remainder Theorem implies that for any $a_1, \ldots, a_n \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \in a_1 \bmod n_1, \quad x = a_2 \bmod n_2, \quad \ldots, \quad x = a_k \bmod n_k$$

and that the solution x is unique mod $n = n_1 n_2 \ldots n_k$.

b) Let $n_i' = n/n_i$ be the quotient of n by n_i, which is relatively prime to n_i by assumption. Let t_i be the inverse of n_i' mod n_i. Prove that the solution x in (a) is given by

$$x = a_1 t_1 n_1' + a_2 t_2 n_2' + \cdots + a_k t_k n_k' \bmod n$$

Note that the elements t_i can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = \gcd(n_i, n_i') = 1$ give $t_i = b$) and that these then quickly give the solutions to the system of congruensces above for any choice of $a_1, a_2, \ldots, a_k$.

c) Solve the simultaneous system of congruences

$$x = 1 \bmod 8, \quad x = 2 \bmod 25, \quad x = 3 \bmod 81$$

and the simultaneous system

$$y = 5 \bmod 8, \quad y = 12 \bmod 25, \quad y = 47 \bmod 81$$

Proof. a) Since the n_i are pairwise coprime, this means that the (n_i) are pairwise comaximal. Using the Chinese Remainder Theorem, we get a surjective map $\varphi : \mathbb{Z} \to \prod \mathbb{Z}/(n_i)$ which has $(\prod n_i)$ for its kernel. Let $(a_i) \in \prod \mathbb{Z}/(n_i)$. Since φ is surjective, then there exists an element $x \in \mathbb{Z}$, where $\varphi(x) = (a_i)$. Using the First Isomorphism Theorem, we see that this x is unique up to mod $\prod n_i$.

b) We see that $\varphi(x) = (\sum a_i t_i n_i')$. We see that the jth coordinate of $\varphi(x)$ is $\sum a_i t_i n_i'$ mod n_j. By the definition of n_i', we see that n_j divides n_i' for all $i \neq j$. Thus, the jth coordinate of $\varphi(x) = a_j t_j n_j' = a_j$ mod n_j, as t_j was defined as the inverse of n_j' mod n_j. This proves that $\varphi(x) = (a_i)$, which proves the statement.

c) We see that $n_1 = 8$, $n_2 = 25$, and $n_3 = 81$ are definitely pairwise coprime. Let $n_1' = 25 \cdot 81$, $n_2' = 8 \cdot 81$, and $n_3' = 8 \cdot 25$. Since $n_1' = 1 \mod 8$, $n_2' = 23 = -2 \mod 25$, and $n_3' = 38 \mod 81$, this means that $t_1 = 1$, $t_2 = 12$, and $t_3 = 32$ as $38 \cdot 32 - 15 \cdot 81 = 1$. This means that $x = 1 \cdot 1 \cdot 25 \cdot 81 + 2 \cdot 12 \cdot 8 \cdot 81 + 3 \cdot 32 \cdot 8 \cdot 25 = 4377 \mod 8 \cdot 25 \cdot 81$.

Using the same constants, we see that $y = 5 \cdot 1 \cdot 25 \cdot 81 + 12 \cdot 12 \cdot 8 \cdot 81 + 47 \cdot 32 \cdot 8 \cdot 25 = 15437 \mod 8 \cdot 25 \cdot 81$.

$\square$

Ex 7 Let m and n be positive integers with n dividing m. Prove that the natural surjective ring projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units: $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. [Incomplete] $\square$

Additional Problems

Ex A A commutative ring R with 1 is said to Noetherian if it has the property that every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

eventually stabilizes. That is, if there is a $N > 0$ such that $I_k = I_N$ for all $k \geq N$. Prove that every PID is Noetherian.

Proof. Let R be a PID, and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals. Then $I = \cup_{i \in \mathbb{N}} I_i$ is also an ideal. Since R is a PID, this means that $I = (\alpha)$ for some $\alpha \in R$. Since $\alpha \in I = \cup_{i \in \mathbb{N}} I_i$ then there is an N such that $\alpha \in I_N$. Let $k \geq N$. Then, this means that $\alpha \in I_k$, which proves that $I \subseteq I_k$. Since $I_k \subseteq I$ by the definition of I, this proves that $I_k = I = I_N$ for all $k \geq N$. $\square$

Ex B Prove that a commutative ring R with 1 is Noetherian if and only if every nonempty set of ideals in R has a maximal element (where as usual the partial ordering is given by inclusion).

Proof. Suppose R is a commutative ring with 1 where every nonempty set of ideals has a maximal element. Let $I_1 \subseteq I_2 \subseteq \dots$ be a chain of ideals. This means that there must be a maximal element among $\{I_i\}_{i \in \mathbb{N}}$, say I_N. Since I_N is maximal, for all $k \geq N$, we see that $I_k \subseteq I_N$ and since $\{I_i\}_{i \in \mathbb{N}}$ is a chain, we also get that $I_N \subseteq I_k$. This proves that $I_N = I_k$ for all $k \geq N$, and thus that R is Notherian.

Now suppose that R is a commutative Notherian Ring with 1, and let $S = \{I_\alpha\}_{\alpha \in A}$ be a nonempty set of ideals. Let $\{I_i\}_{i \in \mathbb{N}}$ be a chain under inclusion in S. Since R is Notherian, there is an N such that $I_N = I_k$ for all $k \geq N$. Thus, I_N is an upper bound of this chain. By Zorn's Lemma, this proves that there is a maximal element in S, and thus that every nonempty set of ideals in R has a maximal element. $\square$

Ex C Prove that a commutative Ring R with 1 is Noetherian if and only if every ideal is finitely generated.

Proof. Let R be a commutative Ring with 1 where every ideal is finitely generated, and let $I_1 \subseteq I_2 \subseteq \ldots$ be a chain of ideals in R. Let $I = \cup_{i \in \mathbb{N}} I_i$. We've already proven before that I is an ideal of R. Since every ideal in R is finitely generated, this means that $I = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ for some $k \in \mathbb{N}$. This means that there are ideals I_{n_i} such that $\alpha_i \in I_{n_i}$ for $1 \leq i \leq k$. Since all these ideals fall on a chain, the union of all of them is one of the elements themselves. Let I_N be this element. Since $\alpha_1, \ldots, \alpha_k \in I_N$, this means that $I \subseteq I_N$ and thus that $I = I_N$. The same is true for all I_k where $k \geq N$. This proves that $I_k = I = I_N$ for all $k \geq N$, and thus that R is Noetherian.

Let R be a commutative Noetherian ring with 1 and let $I \leq R$ be an ideal with no finite generating set. Let $a_1 \in I$. Since I has no finite generating set, this means that $I \setminus (a_i)$ is nonempty. Let $a_2 \in I \setminus (a_i)$. Similarly, let $a_3 \in I \setminus (a_1, a_2)$, and so on. We see that

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$$

is a an ascending chain of ideals. Since R is Noetherian, this means that for some N, $(a_1, a_2, \ldots, a_N) = (a_1, a_2, \ldots, a_k)$ for all $k \geq N$. However, we specifically picked a_k for all $k \geq N$ to not be in $(a_1, a_2, \ldots, a_N)$. This is a contradiction. Thus, I must be finitely generated. $\square$