Math 100B: Homework 1

Merrick Qiu

1. (Artin 11.1.7(a))

Let $A^C = U - A$ be the complement of A. Addition is defined as the symmetric difference, which can be expressed as

$$A + B = A \cup B - A \cap B = (A \cap B^C) \cup (A^C \cap B).$$

Addition is commutative since

$$A + B = (A \cap B^C) \cup (A^C \cap B) = (B \cap A^C) \cup (B^C \cap A) = B + A.$$

Addition is associative since

$$\begin{aligned}
(A + B) + C &= ((A \cap B^C) \cup (A^C \cap B)) + C \\
&= ((A \cap B^C) \cup (A^C \cap B)) \cap C^C \cup ((A \cap B^C) \cup (A^C \cap B))^C \cap C \\
&= (A \cap B \cap C) \cup (A \cap B^C \cap C^C) \cup (A^C \cap B \cap C^C) \cup (A^C \cap B^C \cap C) \\
&= A \cap ((B \cap C^C) \cup (B^C \cap C))^C \cup A^C \cap ((B \cap C^C) \cup (B^C \cap C)) \\
&= A + ((B \cap C^C) \cup (B^C \cap C)) \\
&= A + (B + C).
\end{aligned}$$

The empty set is the additive identity since

$$A + \emptyset = A \cup \emptyset - A \cap \emptyset = A.$$

Each element has itself as its additive inverse since

$$A + A = A \cup A - A \cap A = \emptyset.$$

Multiplication is commutative and associative since intersection is commutative and associative. U is the multiplicative identity since any set intersection with U is itself.

The distributive law holds since

$$\begin{aligned}
(A + B)C &= (A \cup B - A \cap B) \cap C \\
&= (A \cup B) \cap C - A \cap B \cap C \\
&= (A \cap C) \cup (B \cap C) - A \cap C \cap B \cap C \\
&= (A \cap C) + (B \cap C) \\
&= AC + BC
\end{aligned}$$

R is a ring because it satisfies all of the axioms.

2. (Artin 11.1.6(a))

Since $\mathbb{Q}$ is a ring we just need to check that S is closed under subtraction, multiplication, and contains 1. Let $\frac{a}{b}$ and $\frac{c}{d}$ be two elements in S where b and d are not divisible by 3.

S is closed under subtraction and multiplication since the result can be written with denominator bd which is also not divisible by 3.

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - cb}{bd}.$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

S also contains 1 since $1 = \frac{1}{1}$. Therefore S is a subring.

3. (Artin 11.1.9)

Addition is commutative if multiplication is commutative and distributivity holds since

$$\begin{aligned} ab &= ab + 0b \\ &= (a+0)b \\ &= b(a+0) \\ &= ba + b0 \\ &= ba. \end{aligned}$$

4.

If $a^n = 0$, then $(1-a)^{-1} = 1 + a + \ldots + a^{n-2} + a^{n-1}$ since

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

5.

The identities are $f(x) = 0$ and $f(x) = 1$. The units are functions that are not equal to 0 at any point since their inverse is $[f^{-1}](x) = (f(x))^{-1}$. The only nilpotent function is $f(x) = 0$. The zero-divisors are the nonzero functions that are equal to 0 at some point. If f is a function with this property we can define

$$g(x) = \begin{cases} 1 & f(x) = 0 \\ 0 & f(x) \neq 0 \end{cases}$$

so that $g \neq 0$ but $fg = 0$.

Since all functions are either 0 at some point or at no points, all functions are either a zero-divisor or a unit.

6.

The units are the numbers with a multiplicative inverse, which holds for a when $\gcd(a, n) = 1$. The nilpotent elements are the numbers whose prime factors contain the prime factors of n. For example if $n = 242 = 2 \cdot 11^2$ then $a = 132 = 2^2 \cdot 3 \cdot 11$ is a nilpotent element since it contains the prime factors 2 and 11. We can see that $132^2 \equiv 17424 \equiv 0 \mod 242$. The zero-dvisors are the numbers that divide n, which holds for a when $\gcd(a, n) \neq 1$.

Since all numbers either have a gcd of 1 or not 1, all elements are either a unit or a zero-divisor.

7.

(a) Since $\sqrt{r} \notin \mathbb{Q}$, there does not exist $\sqrt{r} = \frac{a}{b}$ for $a, b \in \mathbb{Q}$. Therefore $a_2\sqrt{r}$ and $b_2\sqrt{r}$ are irrational too while a_1 and b_1 are rational. Therefore if $a_1 + a_2\sqrt{r} = b_1 + b_2\sqrt{r}$, then it must be that $a_1 = b_1$ and $a_2 = b_2$.

(b) Subtraction is closed since

$$(a_1 + a_2\sqrt{r}) - (b_1 + b_2\sqrt{r}) = (a_1 - b_1) + (a_2 - b_2)\sqrt{r} \in \mathbb{Q}[\sqrt{r}]$$

Multiplication is closed since

$$(a_1 + a_2\sqrt{r})(b_1 + b_2\sqrt{r}) = (a_1b_1 + a_2b_2r) + (a_1b_2 + a_2b_1)\sqrt{r} \in \mathbb{Q}[\sqrt{r}]$$

The element $1 = 1 + 0\sqrt{r}$ is the multiplicative identity.

The inverse of an element $a_1 + a_2\sqrt{r}$ is $\frac{1}{a_1^2 + a_2^2 r}(a_1 - a_2\sqrt{r})$ since

$$\frac{1}{a_1^2 + a_2^2 r}(a_1 - a_2\sqrt{r})(a_1 + a_2\sqrt{r}) = \frac{1}{a_1^2 + a_2^2 r}(a_1^2 + a_2^2 r) = 1$$

Therefore $\mathbb{Q}[\sqrt{r}]$ is a subfield.

8.

We can perform polynomial long division.

$$
\begin{array}{r}
x^3 \quad + 4x^2 \quad - x \quad - 9 \\
x^2 + 3 \overline{\big) \; x^5 + 4x^4 + 2x^3 \quad + 3x^2 \qquad\qquad} \\
\underline{- x^5 \qquad\quad - 3x^3} \qquad\qquad\qquad\quad \\
4x^4 \quad - x^3 \quad + 3x^2 \qquad\qquad \\
\underline{- 4x^4 \qquad\qquad - 12x^2} \qquad\qquad \\
- x^3 \quad - 9x^2 \qquad\qquad \\
\underline{x^3 \qquad\quad + 3x} \qquad \\
- 9x^2 + 3x \qquad \\
\underline{9x^2 \qquad\quad + 27} \\
3x + 27
\end{array}
$$

Therefore $q(x) = x^3 + 4x^2 - x - 9$ and $r(x) = 3x + 27$. $r(x) = 0$ when $n = 1, 3$.