

# Mathematics GU4042 Modern Algebra II

## Assignment # 5

Benjamin Church

February 16, 2020

**Page 159.**

1. Let  $\{F_i \mid i \in I\}$  be an indexed family of subfields of  $K$ . The set

$$F = \bigcap_{i \in I} F_i$$

is contained in  $K$  so the associative, commutative, and distributive properties are inherited from the field properties of  $K$ . It suffices to check that  $F$  contains 0 and 1 and is closed under addition, multiplication, and inverses. Since every  $F_i$  is a field, each  $F_i$  satisfies these properties. In particular,  $0, 1 \in F_i$ . Also if  $x, y \in F$  then by the definition of the intersection,  $x, y \in F_i$  for every  $i \in I$ . Thus,  $x + y, xy, -x, x^{-1} \in F_i$ . Since this holds for every  $i \in I$  then these elements also appear in the intersection. Thus,  $x + y, xy, -x, x^{-1} \in F$  so  $F$  is a field.

3. Let  $K, L, M$  be subfields of  $F$ . Consider the subfield  $K(LM)$  which is the smallest subfield of  $F$  which contains  $K$  and  $LM$ . Similarly,  $LM \supset L$  and  $LM \supset M$  therefore,  $K(LM)$  contains  $K, L$ , and  $M$ . By the definition of the compositum, any subfield that contains  $K$  and  $L$  must contain  $KL$  because  $KL$  is the intersection of all such subfields. Therefore,  $K(LM) \supset KL$  but  $K(LM)$  also contains  $M$  so by identical reasoning,  $K(LM) \supset (KL)M$ .

The converse proceeds identically. The field  $(KL)M$  contains both the fields  $KL$  and  $M$ . Also,  $KL$  contains  $K$  and  $L$ . Thus,  $(KL)M$  contains  $K, L$ , and  $M$ . Thus, because  $LM$  is the minimal field containing  $L$  and  $M$ ,  $(KL)M \supset LM$ . However,  $(KL)M \supset K$  so  $(KL)M \supset K(LM)$ . Therefore,  $(KL)M = K(LM)$ .

**Page 163.**

7. Let  $F = \mathbb{Z}/2\mathbb{Z}$  which is a field because 2 is a prime. I claim that  $f = X^2 + X + 1$  has no roots in  $F$ . This is easily checked because  $F$  is finite:  $f(0) = 0^2 + 0 + 1 = 1 \pmod{2}$  and  $f(1) = 1^2 + 1 + 1 = 1 \pmod{2}$ . From problem # 9 on assignment # 3, we know that any degree two polynomial over  $F$  is irreducible iff it has no roots in  $F$ . Thus,  $f$  is irreducible over  $F$  and therefore,  $E = F[X]/(X^2 + X + 1)$  is a field. We know that  $[E : F] = 2$  because  $\deg f = 2$  with  $\{1, X\}$  forming a basis of  $E$  over  $F$ . Since  $F$  contains 2 elements,  $E$  contains 4 elements, namely,  $0, 1, X, 1 + X$ . We explicitly exhibit their addition and multiplication tables below.

Addition				
	0	1	$X$	$1 + X$
0	0	1	$X$	$1 + X$
1	1	0	$1 + X$	$X$
$X$	$X$	$1 + X$	0	1
$1 + X$	$1 + X$	$X$	1	0

Multiplication				
	0	1	$X$	$1 + X$
0	0	0	0	0
1	0	1	$X$	$1 + X$
$X$	0	$X$	$1 + X$	1
$1 + X$	0	$1 + X$	1	$X$

$(E, +) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and  $(E^\times, \cdot) \cong \mathbb{Z}/3\mathbb{Z}$ .

4. Let  $S = \{i, \sqrt{2}\}$  and consider  $\mathbb{Q}(S) \subset \mathbb{C}$ . By definition,  $\mathbb{Q}(S)$  must contain  $\mathbb{Q}, i$  and  $\sqrt{2}$  and thus by closure,  $\mathbb{Q}(S)$  must contain  $i\sqrt{2}$  and all  $\mathbb{Q}$ -linear combinations of the elements  $\{1, i, \sqrt{2}, i\sqrt{2}\}$ . If we prove that the set of all such combinations,  $L$ , is a field, then it must be  $\mathbb{Q}(S)$  because  $\mathbb{Q}(S)$  is the smallest field containing this set.

Clearly,  $L$  is closed under addition and contains additive inverses. It remains to check multiplicative closure and inverses. Take  $x, y \in L$  then  $x = a + ib + c\sqrt{2} + id\sqrt{2}$  and  $y = a' + ib' + c'\sqrt{2} + id'\sqrt{2}$  with constants in  $\mathbb{Q}$ . Now,

$$\begin{aligned}
xy &= aa' + iab' + ac'\sqrt{2} + iad'\sqrt{2} + iba' - bb' + ibc'\sqrt{2} - bd\sqrt{2} \\
&\quad + ca'\sqrt{2} + icb'\sqrt{2} + 2cc' + 2icd' + ida'\sqrt{2} - db'\sqrt{2} + 2idc' - 2dd' \\
&= (aa' - bb' + 2cc' - dd') + i(ab' + ba' + 2cd' + 2idc') \\
&\quad + (ac' - bd + ca' - db')\sqrt{2} + i(ad' + bc' + cb' + da')\sqrt{2} \in L
\end{aligned}$$

Thus,  $L$  is closed under multiplication. It remains to prove that  $L$  contains multiplicative inverses.

$$\begin{aligned}
x^{-1} &= \frac{1}{(a + c\sqrt{2}) + i(b + d\sqrt{2})} = \frac{(a + c\sqrt{2}) - i(b + d\sqrt{2})}{(a + c\sqrt{2})^2 + (b + d\sqrt{2})^2} \\
&= \frac{(a + c\sqrt{2}) - i(b + d\sqrt{2})}{(a^2 + b^2 + c^2 + d^2) + (2ac + 2bd)\sqrt{2}} \\
&= \frac{[(a + c\sqrt{2}) - i(b + d\sqrt{2})] [(a^2 + b^2 + c^2 + d^2) - (2ac + 2bd)\sqrt{2}]}{(a^2 + b^2 + c^2 + d^2)^2 - 2(2ac + 2bd)^2} \in L
\end{aligned}$$

The final inclusion holds because by closure under multiplication the numerator is in  $L$  and the denominator is in  $\mathbb{Q}$ . Furthermore, the denominator cannot be zero unless

$$(a^2 + b^2 + c^2 + d^2)/(2ac + 2bd) = \sqrt{2}$$

which is impossible because  $\sqrt{2}$  is irrational. Thus,  $L$  is a field containing  $\mathbb{Q}, i, \sqrt{2}$  with  $L \subset \mathbb{Q}(S)$  and therefore  $\mathbb{Q}(S) = L$ . Furthermore, the set we have exhibited is a basis of  $\mathbb{Q}(S)$  over  $\mathbb{Q}$ . By the definition of  $L = \mathbb{Q}(S)$ , the set  $B = \{1, i, \sqrt{2}, i\sqrt{2}\}$  spans  $\mathbb{Q}(S)$ . Suppose that

$$a + ib + c\sqrt{2} + id\sqrt{2} = 0$$

then by properties of complex numbers,

$$a + c\sqrt{2} = 0 \text{ and } b + d\sqrt{2} = 0$$

However, if  $c \neq 0$  then  $\sqrt{2} = -\frac{a}{c} \in \mathbb{Q}$  contradicting its irrationality. Thus,  $c = 0$  so  $a = 0$ . Similarly, if  $d \neq 0$  then  $\sqrt{2} = -\frac{b}{d} \in \mathbb{Q}$  so  $b = d = 0$ . Thus,  $B$  is linearly independent. Therefore,  $B$  is a basis of  $\mathbb{Q}(S)$  over  $\mathbb{Q}$  so  $[\mathbb{Q}(S) : \mathbb{Q}] = 4$ .