NAP 2019, HOMEWORK SET #1, MAY 113, 2019

ROGER & SYLVIA WIEGAND

• 1.1. Let a be an element of a group G. By definition, there is an element $b \in G$ such that $ab = ba = e$. Suppose c also satisfies $ac = ca = e$. Then

$$c = ce = c(ab) = (ca)b = eb = b.$$

(There are many ways to prove this, but this is kind of slick and uses only that c is a left inverse and b is a right inverse.)

• 1.3. Let $x \in G$. If $x \in H$, then $xH = H$. If $x \notin H$, then, since G is the disjoint union of its left cosets, and since there are only two of them, xH must be $G \setminus H$. Similarly, $Hx = H$ if $x \in H$, and $Hx = G \setminus H$ if $x \notin H$. Thus $xH = Hx$ for every $x \in G$, that is, $H \lhd G$.

• 1.4. Let $x \in G$. Then $xHx^{-1} \leq G$. Also, we claim that the function $f : H \to xHx^{-1}$ defined by $f(h) = xhx^{-1}$ is both one-to-one and onto. Obviously it's onto. To see that it's one-to one, suppose $f(h) = f(h')$. Then $xhx^{-1} = xh'x^{-1}$. Multiply both sides on the left by x^{-1} and on the right by x to get $h = h'$. This shows that $|xHx^{-1}| = |H| = k$. Therefore, by the hypothesis, $xHx^{-1} = H$. Since x is an arbitrary element of G, this shows that $H \lhd G$.

[• Although 1.5 was not assigned, it's important and it probably should have been assigned; so we'll give an example here (which we hope you have already found on your own). The Klein 4-group $V := \{(1), (12)(34), (13)(24), (14)(23)\}$ is normal in S_4. (Recall the effect of conjugation on a cycle, or on a product of disjoint cycles; normality follows immediately.) Also, $H := \{(1), (12)(34)\}$ is normal in V, since it has index 2. But H is not a normal subgroup of S_4, since $(13)\big((12)(34)\big)(13)^{-1} = (32)(14) = (14)(23)$, which is not in H.]

• 1.6. Since every permutation can be written as a product of cycles (in fact, disjoint cycles), it's enough to show that every cycle is a product of transpositions. Here goes: $(a_1\ a_2\ \dots a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2)$. (What a nuisance, having to start on the right!)

• 1.12. To show well-definedness, suppose $a + n\mathbb{Z} = a' + n\mathbb{Z}$ and $b + n\mathbb{Z} = b' + n\mathbb{Z}$. We have to show that $ab + n\mathbb{Z} = a'b' + n\mathbb{Z}$. We have $a - a' \in n\mathbb{Z}$ and $b - b' \in n\mathbb{Z}$; therefore $(ab - a'b') = a(b - b') + (a - a')b'$, which is in $n\mathbb{Z}$ (by the "sponge property and closure under addition). Therefore $ab - a'b' \in n\mathbb{Z}$, that is, $ab + n\mathbb{Z} = a'b' + n\mathbb{Z}$.

If $n = 1$ then $\mathbb{Z}_n$ has only one element, so it's not a field. Assume $n \geq 2$. If n is not a prime, let $n = ab$, where $1 < a \leq b < n$. If $\mathbb{Z}_n$ were a field, the non-zero element $a + \mathbb{Z}$ would have to have an inverse, say, $ac \equiv 1$ (where "$\equiv$" denotes "$\equiv \pmod n$"). But $ab \equiv 0$, and hence $b \equiv bac \equiv 0c \equiv 0$, which is false, since $1 < b < n$. Thus $\mathbb{Z}_n$ is not a field.

Finally we show $\mathbb{Z}_p$ is a field if p is a prime. The associative and distributive laws all follow from those in $\mathbb{Z}$, so we just have to show that every non-zero element $a + p\mathbb{Z}$ has an inverse. We may assume that $0 < a < p$. Then a and p are relatively prime. By the Euclidean algorithm, their greatest common divisor, namely 1, can be expressed in the form $ax + py$. Then $1 = ax + py$, and hence $ax \equiv 1$. Thus $(a + p\mathbb{Z})(x + p\mathbb{Z}) = 1$, and we have found the inverse of $a + p\mathbb{Z}$. Hurray!

• 1.13. They are all closed under addition and subtraction, so we just have to check closure under multiplication, and existence of inverses.

(i) is a subfield. $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, and $(a+bi)\frac{a-bi}{a^2+b^2} = 1$, as long as a and b are not both equal to 0.

(ii) One checks directly that $\omega^2 = -(\omega+1)$. Therefore $(a+b\omega)(c+d\omega) = ac - bd(\omega+1) + (ad+bc)\omega = (ac-bd) + (ad+bc-bd)\omega$. For inverses, if a and b are not both 0, we want to find c, d so that $(a+b\omega)(c+d\omega) = 1$. It makes sense to use the conjugate $\overline{\omega} = \frac{1}{2}(-1-\sqrt{3}i)$, which satisfies $\omega\overline{\omega} = 1$ and $\omega + \overline{\omega} = -1$. Therefore $(a+b\omega)(a+b\overline{\omega}) = a^2 - ab + b^2$. Then, as long as $a^2 - ab + b^2 \neq 0$, we have $(a+b\omega)^{-1} = \frac{a+b\overline{\omega}}{a^2-ab+b^2}$. We just have to show that $a^2 - ab + b^2 \neq 0$ unless a and b are both 0. If $a = 0$ and $b \neq 0$, this is trivial, so assume that $a \neq 0$. If, now, $a^2 - ab + b^2 = 0$, we have $1 - \frac{b}{a} + (\frac{b}{a})^2$, which is impossible since $1 - x + x^2$ has no rational roots.

(iii) Put $\beta = 2^{\frac{1}{3}}$. The subset of $\mathbb{C}$ we are to analyze is $V := \{a + b\beta \mid a, b \in \mathbb{Q}\}$. This is *not* a subfield of $\mathbb{C}$ because it is not closed under multiplication. In fact, $\beta^2 \notin V$. To see this, suppose that we have

eq:belch

$$\beta^2 = a + b\beta \quad \text{with} \quad a, b \in \mathbb{Q}\,. \tag{0.1}$$

Let $g(x) = x^3 - 2$ and $f(x) = x^2 - bx - a \in \mathbb{Q}[x]$. Notice that $g(\beta) = 0$ and $f(\beta) = 0$. Using long division (dividing by $g(x)$ by $f(x)$), we get

$$g(x) = f(x)q(x) + r(x), \quad \text{where} \quad q(x) = x + b \quad \text{and} \quad r(x) = (a+b^2)x + (ab-2)\,.$$

Setting $x = \beta$, we see that $r(\beta) = 0$, that is,

eq:snort

$$(a+b^2)\beta + (ab-2) = 0\,. \tag{0.2}$$

If $a + b^2 = 0$, then $ab - 2 = 0$ too, and it would follow that a and b are both negative, which would contradict Equation (0.1). Therefore $a + b^2 \neq 0$, and we can divide by $a + b^2$ in Equation (0.2) and get $\beta \in \mathbb{Q}$. But this is false, and we're done (except for showing that β is irrational). The proof that β is irrational is just like the proof that $\sqrt{2}$ is irrational: Write $\beta = \frac{r}{s}$, where r and s are relatively prime positive integers. Then $2 = \frac{r^3}{s^3}$, so $2s^3 = r^3$. Therefore r is even, say $r = 2t$. Now we get $2s^3 = 8t^3$, so $s^3 = 4t^3$. Therefore s is even too, a contradiction.

By next week, after a little theory has been developed, you'll be able to do problems like this very easily!

(iv) This one is a subfield. Closure under multiplication is easy. A direct proof of the existence of inverses is a mess, so we will use a little bit of cleverness. Note that the set (call it R) is a three-dimensional vector space over $\mathbb{Q}$. If γ is a non-zero element of R, consider the linear transformation $f : R \to R$ given by multiplication by γ: $f(x) = \gamma x$ for every $x \in R$. Since R is a subring of $\mathbb{C}$ (in fact, of $\mathbb{R}$) we see that $\operatorname{Ker} f = 0$. Thus f is an injective linear transformation of a finite-dimensional vector space and hence is surjective. Thus there is some element $\delta \in R$ such that $f(\delta) = 1$, that is, $\gamma\delta = 1$. Amazing! We have shown tht γ has an inverse.

• 1.16. We will dutifully follow the directives given in the notes from Class 3.

(1) Since $2^{n+1} > 2^n$ for every $n \geq 0$, it follows from **Fact 1** that $\boldsymbol{u}_{n+1}$ is not in the subfield generated by $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ and *a fortiori* not in the $\mathbb{Q}$-linear subspace spanned by $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$. Thus $\boldsymbol{u}_1 \notin \mathbb{Q}$ and, for each $n \geq 1$, $\boldsymbol{u}_{n+1}$ is not a linear combination of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$. Using this observation, we show that every finite subset F of the infinite set $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \ldots\}$ is linearly independent over $\mathbb{Q}$. Choose n big enough so that F is contained in $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$. It will suffice to show that

$\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ is linearly independent, since any subset of a linearly independent set is linearly independent. Suppose $c_i \in \mathbb{Q}$ and $c_1\boldsymbol{u}_1 + \cdots + c_n\boldsymbol{u}_n = 0$ with not all $c_i = 0$. Let c_m be the last non-zero coefficient, that is, $c_m \neq 0$ but $c_i = 0$ for $m < i \leq n$. By dividing by c_m, we can express $\boldsymbol{u}_m$ as a linear combination of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m-1}$, contradicting the observation we made above. This proves linear independence.

(2) The proof is *exactly* the same as for (1), except for substitution of "$\boldsymbol{w}$" for "$\boldsymbol{u}$" everywhere.

(3) Suppose $a\sqrt{2} + b\sqrt{3} + c\sqrt{5} = 0$, with $a, b, c \in \mathbb{Q}$. We have to show that $a = b = c = 0$. Writing this equation three ways, and then squaring both sides, we obtain the following equations:

$$-a\sqrt{2} = b\sqrt{3} + c\sqrt{5} \quad \implies \quad 2a^2 = 3b^2 + 2bc\sqrt{15} + 5c^2$$
$$-b\sqrt{3} = a\sqrt{2} + c\sqrt{5} \quad \implies \quad 3b^2 = 2a^2 + 2ac\sqrt{10} + 5c^2$$
$$-c\sqrt{5} = a\sqrt{2} + b\sqrt{3} \quad \implies \quad 5c^2 = 2a^2 + 2ab\sqrt{6} + 3b^2$$

Examining the equations on the right, we see that $bc \neq 0 \implies \sqrt{15} \in \mathbb{Q}$, $ac \neq 0 \implies \sqrt{10} \in \mathbb{Q}$, and $ab = 0 \implies \sqrt{6} \in \mathbb{Q}$. Therefore we must have $bc = ac = ab = 0$. Hence, if $a \neq 0$ we'd have $b = c = 0$, which would imply that $a\sqrt{2} = 0$, a contradiction. Similarly, $b \neq 0$ would imply $b\sqrt{3} = 0$, and $c \neq 0$ would imply $c\sqrt{5} = 0$, both of which are contradictions. Thus $a = b = c = 0$.

• 1.17 (as modified in the notes on Class #1)

(a) Suppose $V = U_1 \cup \cdots \cup U_n$, where the U_i are proper subspaces of the 2-dimensional vector space V over the infinite field K. We can toss out any of the U_i that happen to be $\{0\}$, so we assume that each U_i has dimension one. Let $\{\boldsymbol{v}, \boldsymbol{w}\}$ be a basis of V. Choose $n + 1$ distinct elements $c_1, \ldots c_{n+1} \in K$, and choose, for each $i = 1, \ldots, n+1$, one of the given one-dimensional subspaces that contains the vector $\boldsymbol{v}+c_i\boldsymbol{w}$. Since $n+1 > n$, two of these elements must lie in the *same* one-dimensional subspace. This means that $\boldsymbol{v} + c_i\boldsymbol{w}$ and $\boldsymbol{v} + c_j\boldsymbol{w}$ are in a one-dimensional subspace U_i. Then

$$\boldsymbol{v} + c_i\boldsymbol{w} - (\boldsymbol{v} + c_j\boldsymbol{w}) \in U_i \implies (c_i - c_j)\boldsymbol{w} \in U_i \implies \boldsymbol{w} \in U_i \text{ and } \boldsymbol{v} \in U_i,$$

since we had $\boldsymbol{v} + c_i\boldsymbol{w} \in U_i$. This contradicts $\dim U_i = 1$.

(b) Let $K = \{0, 1\}$, the two-element field. Let V be a two-dimensional vector space over K with a basis $\{\boldsymbol{v}, \boldsymbol{w}\}$. Then V has just four elements, namely, $\mathbf{0}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{v} + \boldsymbol{w}$. Now notice that V is the union of the three one-dimensional subspaces $\{\mathbf{0}, \boldsymbol{v}\}$, $\{\mathbf{0}, \boldsymbol{w}\}$, and $\{\mathbf{0}, \boldsymbol{v} + \boldsymbol{w}\}$.