ANSWERS TO SOME OF THE HOMEWORK PROBLEMS

Tenth problem set

1. First, by the quadratic formula, the roots of x^2+x+1 are $-\frac{1}{2}\pm\frac{1}{2}\sqrt{-3}$, both of which lie in $\mathbb{Q}(\sqrt{-3})$ but not in $\mathbb{Z}[\sqrt{-3}]$. In particular, x^2+x+1 is reducible in $\mathbb{Q}(\sqrt{-3})$ since it has a root. Now suppose that there is a factorization $x^2+x+1=(ax+b)(cx+d)$ with $a,b,c,d\in\mathbb{Z}[\sqrt{-3}]$. Then $x^2=acx^2$, hence a and c are units. In this case, since $ax+b$ is a factor of x^2+x+1, $-a^{-1}b\in\mathbb{Z}[\sqrt{-3}]$ is a root of x^2+x+1, contradicting the fact that there is no root of x^2+x+1 in $\mathbb{Z}[\sqrt{-3}]$. Finally, if $x^2+x+1=rg(x)$, where $g(x)\in\mathbb{Z}[\sqrt{-3}][x]$ has degree 2, then $1=ra$ for some $a\in\mathbb{Z}[\sqrt{-3}]$, hence r is a unit. Thus x^2+x+1 is irreducible in $\mathbb{Z}[\sqrt{-3}][x]$ but not in $\mathbb{Q}(\sqrt{-3})[x]$.

2. (a) Irreducible in $\mathbb{Q}[x]$ since Eisenstein at 5, but is equal to $2(x^4-25x^3+50x^2-375x+30)$ in $\mathbb{Z}[x]$. (b) Irreducible in $\mathbb{Q}[x]$ by the rational roots test (joy inly need to check ±1) and hence in $\mathbb{Z}[x]$ since monic, hence primitive. (c) It has the rational root $-\frac{1}{2}$, hence $2x+1$ is a factor. The complete factorization is $(2x+1)(x^2+x+1)$, where the second factor is irreducible in $\mathbb{Q}[x]$ as it has no rational root, and in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Q}[x]$ and monic, hence primitive. (e) Reducible in both $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$, complete factorization $(x^2+2)(x^2+3)$. Both factors are irreducible in $\mathbb{Q}[x]$ as they have no rational roots, and in $\mathbb{Z}[x]$ since irreducible in $\mathbb{Q}[x]$ and monic, hence primitive. (f) Irreducible in $\mathbb{Q}[x]$ and complete factorization in $\mathbb{Z}[x]$ given by: $3(x^{27}-28)$. Here $x^{27}-28$ is Eisenstein at 7, hence irreducible in $\mathbb{Q}[x]$ and thus in $\mathbb{Z}[x]$ since primitive.

3. Clearly, if $f(x)=g(x)h(x)$ with $\deg g,\deg h>0$, then $f(ax+b)=g(ax+b)h(ax+b)=G(x)H(x)$, say, with $G(x)=g(ax+b)$ and $H(x)=h(ax+b)$, so $f(x)$ reducible $\implies$ $f(ax+b)$ reducible (note that $\deg g(ax+b)=\deg g(x)$ and similarly for $h(ax+b)$). Conversely, if $f(ax+b)$ is reducible, say $f(ax+b)=G(x)H(x)$, then note that $a(a^{-1}x-a^{-1}b)+b=x$, hence $f(x)=G(a^{-1}x-a^{-1}b)H(a^{-1}x-a^{-1}b)$ and as before this is a nontrivial factorization.

4. Note: although this was omitted, **we must assume that the characteristic of F is not 2 throughout.** (i) First, if $g(x)=x^2+ax+b$ is a factor of $f(x)=x^4+c$, then by the argument of Problem 3 above

$g(-x) = x^2 - ax + b$ is a factor of $f(-x) = f(x)$, and conversely. Hence, if $a \neq 0$, then we have found two distinct factors (since $-a \neq a$).

If $x^2 + b$ is a factor of $x^4 + c$, there is another quadratic factor, say $x^2 + ax + d$. Then

$$(x^2 + b)(x^2 + ax + d) = x^4 + c = x^4 + ax^3 + (b + d)x^2 + abc + bd.$$

Hence $a = 0$ and $b + d = 0$, hence $d = -b$ and $c = -b^2$. So the second quadratic factor is necessarily of the form $x^2 - b$. Next suppose that $f(x) = x^4 + c$ has a linear factor. Then it has a root, say t, with $t^4 = -c$, and hence in particular $-c$ is a square in F. Putting this together, suppose that $f(x)$ is reducible. If it has a linear factor, then $-c$ is a square. So we assume that there is no linear factor. In particular, $c \neq 0$. Now suppose that $f(x)$ is a product of two quadratic polynomials. If the coefficient of x in one factor is zero, then the coefficient of x in both factors is zero and $f(x) = x^4 - b^2$, so that again $-c$ is a square. Conversely, if $-c = b^2$ is a square, then $f(x) = (x^2 + b)(x^2 - b)$. Finally suppose that the coefficient of x in one factor is nonzero, say $x^2 + ax + b$ divides $f(x)$ with $a \neq 0$. Then $x^2 - ax + b$ also divides $f(x)$. Note that the gcd of $x^2 + ax + b$ and $x^2 - ax + b$ divides the difference

$$x^2 + ax + b - (x^2 - ax + b) = 2ax.$$

Hence $x^2 + ax + b$ and $x^2 - ax + b$ are not relatively prime $\iff$ they are both divisible by x, but in this case x is a factor of $x^4 + c$ and $c = 0$, which we have already dealt with. So we may assume that $x^2 + ax + b$ and $x^2 - ax + b$ are relatively prime and both of them divide $f(x)$. Hence (as all polynomials are monic) $x^4 + c = (x^2 + ax + b)(x^2 - ax + b)$. Note that, if

$$x^4 + c = (x^2 + ax + b)(x^2 - ax + b) = x^4 + (2b - a^2)x^2 + b^2,$$

then $c = b^2$ and $2b = a^2$. Conversely, if c is the square of an element $b \in F$ such that $2b = a^2$ for some $a \in F$, then $x^4 + c = (x^2 + ax + b)(x^2 - ax + b)$.

Summarizing, we have shown that $f(x)$ is reducible $\iff$ either $-c$ is a square or c is the square of an element $b \in F$ such that $2b = a^2$ for some $a \in F$. For example,

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

(ii) This is very similar: since $f(x) = x^4 + c_1x^2 + c_2$ satisfies $f(-x) = f(x)$, if if $g(x) = x^2 + ax + b$ is a factor of $f(x)$, then $g(-x) = x^2 - ax + b$ is also a

factor of $f(-x) = f(x)$. (Hence, arguing as in Part (i), if $a \neq 0$ and x does not divide $f(x)$, then $f(x) = (x^2 + ax + b)(x^2 - ax + b)$.) Now assume that $f(x) = (x^2 + ax + b)(x^2 - ax + b)$ (where we allow for the case $a = 0$). Then as before

$$x^4 + c_1x^2 + c_2 = (x^2 + ax + b)(x^2 - ax + b) = x^4 + (2b - a^2)x^2 + b^2,$$

so that $c_2 = b^2$ and $c_1 = 2b - a^2$. Conversely, if c_2 is the square of an element $b \in F$ such that $2b - c_1 = a^2$ for some $a \in F$ (possibly 0), then reversing this procedure we see that $f(x) = (x^2 + ax + b)(x^2 - ax + b)$. (Note that it is usually the case that $2b - c_1$ is a square but that $2(-b) - c_1$ is not a square, so we have to check **both** square roots of c_2.)

(iii) This is just the quadratic formula, which holds in any field F whose characteristic is not 2: $x^4 + c_1x^2 + c_2 = (x^2 + a)(x^2 + b) \iff$ the corresponding quadratic polynomial $x^2 + c_1x + c_2$ factors in $F[x]$ into linear factors $(x + a)(x + b) \iff$ the discriminant $c_1^2 - 4c_2$ is a square in F. (Of course, you can do this directly by retracing the derivation of the quadratic formula as well.)

5. Note that, if $p = 2$, then the reduction $\bar{f}(x)$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ is $x^4 + 1 = (x + 1)^4$ which is reducible. So we only need to look at odd primes p, where the characteristic of $\mathbb{Z}/p\mathbb{Z}$ is not 2, and hence the results of Problem 4 apply.

(i) Here $c_1 = -10$ and $c_2 = 1$, so that 1 is a square with possible square roots ± 1, and $\pm 2 - (-10)$ is either $12 = 2^2 \cdot 3$ or $8 = 2^2 \cdot 2$. So if either 2 or 3 is a square mod p we are in case (ii) of Problem 4.

(ii) Here $c_1^2 - 4c_2 = 100 - 4 = 96 = 2^2 \cdot 6$ which is a square mod $p \iff 6$ is a square mod p.

(iii) By standard results on cyclic groups, if $n = 2k$ is an even positive integer, then $\langle 2 \rangle = 2\mathbb{Z}/n\mathbb{Z}$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order $k = n/\gcd(2, n)$ and hence the index of $\langle 2 \rangle$ in $\mathbb{Z}/n\mathbb{Z}$ is 2. Correspondingly, if G is a (multiplicative) group which is cyclic of order $n = 2k$ and H is the subgroup of G consisting of elements of the form g^2 for $g \in G$, then H is a subgroup of index 2, automatically normal. There are thus two cosets of H in G: the identity coset consists of the squares in G and the remaining coset $G - H$ consists of the elements which are not squares. Moreover the product of two elements in $G - H$ is automatically in H, i.e. is a square. Applying this to the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p - 1$, which is even if $p \neq 2$, we see that if 2 and 3 are not squares then 6 is a square. Hence the image $\bar{f}(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ is reducible for all odd primes p.

(iv) By the rational roots test, a root of $f(x)$ in $\mathbb{Q}$ would have to be ± 1, and direct inspection shows that neither of these is a root. Hence $f(x)$

does not factor as linear times cubic, so it could only factor as a product of two quadratic polynomials. By Problem 5 (ii), $f(x)$ is not of the form $(x^2+ax+b)(x^2-ax+b)$, and hence does not have a quadratic factor of the form x^2+ax+b with $a \neq 0$, since 12 and 8 are not squares in $\mathbb{Q}$ ($\sqrt{2}$ and $\sqrt{3}$ are irrational). The remaining possibility is then that $f(x) = (x^2+a)(x^2+b)$, but this case is not possible since 96 is not a square in $\mathbb{Q}$ ($\sqrt{6}$ is irrational). Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$. (Note: we showed in class by a different method that $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.)

Eleventh problem set

1. Suppose that $r(t) \in F(t)$ and that $r(t)$ is algebraic over F, in other words that there exists a monic polynomial $f(x) \in F[x]$ such that $f(r(t)) = 0$. If $r(t) = 0$, then $r(t) = r \in F$ already, so we can assume that $r(t) \neq 0$. Hence, writing $f(x) = x^k g(x)$, where $g(0) \neq 0$, it follows that $g(r(t)) = 0$ and that the constant term a_0 of $g(x)$ is nonzero. By the rational roots test, writing $r(t) = p(t)/q(t)$ where p and q are relatively prime, and viewing $g(x) \in F[x] \subseteq F(t)[x]$, it follows since $F[t]$ is a UFD with field of quotients $F(t)$ that q divides the leading coefficient 1 of $g(x)$ in $F[t]$ and that p divides the constant term a_0 of $g(x)$ in $F[t]$. Hence $p(t)$ and $q(t)$ are constants and $r(t) = p/q \in F$.

2. Write $f(x) = c(f)f_0(x)$ and $g(x) = c(g)g_0(x)$, where $f_0(x)$ and $g_0(x)$ are primitive. Then $f(x)g(x) = c(f)c(g)(f_0(x)g_0(x))$. By the Gauss lemma, $f_0(x)g_0(x)$ is primitive. Hence the content $c(fg)$ of $f(x)g(x)$ is equal to $c(f)c(g)$.

3. As a homomorphism between two fields, σ is automatically injective. We claim that σ is surjective. Since σ is F-linear, the image $\sigma(E)$ is an F-vector subspace of E. Let $\alpha_1, \ldots, \alpha_n$ be a basis of E. Then we claim that $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are linearly independent over F: if $\sum_{i=1}^n a_i\sigma(\alpha_i) = 0$, then

$$0 = \sum_{i=1}^n a_i\sigma(\alpha_i) = \sigma(\sum_{i=1}^n a_i\alpha_i).$$

Since σ is injective, $\sum_{i=1}^n a_i\alpha_i = 0$, hence $a_i = 0$ for all i since the $\alpha_1, \ldots, \alpha_n$ are linearly independent. Thus the image $\sigma(E)$ of σ is an F-vector subspace of E, and $\dim_F \sigma(E) \geq n = \dim_F E$. Hence $\sigma(E) = E$.

4. Every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be uniquely written as $a + b\sqrt{2} + c\sqrt{3} +$

$d\sqrt{6}$. From

$$\sigma_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6};$$
$$\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6};$$
$$\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6},$$

we see that

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle\sigma_1\rangle} = \mathbb{Q}(\sqrt{3});\ \mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt{2});\ \mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt{6}).$$

5. Since $\omega \notin \mathbb{R}$, hence $\omega \notin \mathbb{Q}(\sqrt[3]{2})$, and ω is the root of a polynomial of degree 2 with coefficients in $\mathbb{Q}$, and hence in $\mathbb{Q}(\sqrt[3]{2})$, $[\mathbb{Q}(\sqrt[3]{2},\omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$ and $1, \omega$ is a basis for $\mathbb{Q}(\sqrt[3]{2},\omega)$ as a $\mathbb{Q}(\sqrt[3]{2})$-vector space. Note that $\bar{\omega} = \omega^2 = -1-\omega$. Every element of $\mathbb{Q}(\sqrt[3]{2},\omega)$ can be uniquely written as $\alpha+\beta\omega$, where $\alpha, \beta \in \mathbb{Q}(\sqrt[3]{2})$ which is a subfield of $\mathbb{R}$. Hence

$$\sigma(\alpha+\beta\omega) = \alpha+\beta\bar{\omega} = \alpha+\beta(-1-\omega) = (\alpha-\beta)+(-\beta)\omega.$$

Thus $\sigma(\alpha+\beta\omega) = \alpha+\beta\omega \iff \alpha-\beta = \alpha$ and $-\beta = \beta \iff \beta = 0$. Hence the fixed field is just $\mathbb{Q}(\sqrt[3]{2})$.

6. (a) Clearly $x^5-1 = (x-1)\Phi_5(x)$ and

$$x^5-1 = (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4).$$

Comparing, we see that the roots of $\Phi_5(x)$ are $\zeta_1 = \zeta, \zeta_2 = \zeta^2, \zeta_3 = \zeta^3, \zeta_4 = \zeta^4$. Since $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1,\zeta_2,\zeta_3,\zeta_4)$ is generated by the roots of $\Phi_5(x)$, the action of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ on the set $\{\zeta_1,\zeta_2,\zeta_3,\zeta_4\}$ defines an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to S_4. (b) Given $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, once we know $\sigma(\zeta)$, then $\sigma(\zeta_i) = \sigma(\zeta^i) = (\sigma(\zeta))^i$. Hence there are at most 4 possibilities for σ.

7. If σ is an automorphism of $\mathbb{R}$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$, consider $\sigma(\sqrt[4]{2}) \in \mathbb{R}$. Then $(\sigma(\sqrt[4]{2}))^2 > 0$ since it is a positive real number. But

$$(\sigma(\sqrt[4]{2}))^2 = \sigma((\sqrt[4]{2})^2) = \sigma(\sqrt{2}) = -\sqrt{2} < 0,$$

a contradiction.